

Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Návrh antény pro aplikace RFID v pásmu HF
Antenna design for HF RFID applications

2019/2020

Bc. Marianna Mikulecká

Zadání diplomové práce

Student: **Bc. Marianna Mikulecká**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T059 Mobilní technologie

Téma: **Návrh antény pro aplikace RFID v pásmu HF.**
Antenna Design for HF RFID Applications

Jazyk vypracování: čeština

Zásady pro vypracování:

Navrhněte a vyhodnoťte funkčnost antény určené pro čtečky RFID. Rozměry antény musí odpovídat prostorovým nárokům zařízení, pro které se bude anténa používat. Přesnou frekvenci a limitní rozměry antény dodá vedoucí diplomové práce.

Hlavní propozice práce:

1. Popište typy antén pro aplikace RFID.
2. Navrhněte geometrii antény pro předepsané zástavbové rozměry.
3. Simulujte anténu včetně připojovacího konektoru programem CST Microwave studio. Proved'te optimalizaci tvaru antény.
4. Vyřešte připojení antény k obvodům napájení.
5. Vytvořte anténu a ověřte její funkčnost měření.

Seznam doporučené odborné literatury:

[1] Laheurte, J., Ripoll, Ch., Paret, D., Loussert, Ch.: UHF RFID Technologies for identification and Traceability, Wiley, 2014, ISBN 978-1-84821-592-4


Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.


Vedoucí diplomové práce: **doc. Ing. Lubomír Ivánek, CSc.**

Datum zadání: 01.09.2018

Datum odevzdání: 30.04.2020




prof. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry


prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě dne: *15. května 2020*



podpis studenta

Poděkování

Ráda bych poděkovala panu doc. Ing. Lubomíru Ivánkovi, CSc. za odborné vedení, pomoc a konzultace při vytváření této diplomové práce, panu Ing. Marku Dvorskému, Ph.D. za odborné rady, Miroslavu Schneiderovi, Ing. a panu Ing. Petru Orságovi, Ph.D. za pomoc při měření. Dále bych poděkovala panu Ing. Zdeňku Králíkovi za pomoc a umožnění náhradního měření. A děkuji své rodině a přátelům za podporu.

Abstrakt

První zadání bylo zaměřené pouze na biometrické pasy a konstrukci RFID antény pro čtení biometrických pasů. Jedná se o antény ve vysokofrekvenčním pásmu na kmitočtu 13,56 MHz. Při studiu jsem zjistila, že problematika je tak široká a pestrá, že nelze oddělit jen tuto část a soustředit se pouze na ní. Tyto antény nevyrábí každý, protože se dodávají se specializovaným softwarem, který musí zvládat šifrování, ověřování digitálních podpisů atp. Boj proti padělání pasů vyžaduje, aby k těmto technologiím měly přístup jen certifikované a prověřené firmy. Nepodařilo se mi zajistit praktické ověření funkce mé antény na reálném zařízení. Proto jsem anténu musela zkoušet a ladit na komerčně vyráběné čtečce, na které jsem ale přes veškerou snahu nedokázala přečíst ani pas, ani občanský průkaz. Zvolila jsem poměrně neobvyklou konstrukci antény – diferenciální. Nelze ji změřit běžným spektrálním analyzátozem, protože nemá dva vstupy a musela se měřit pouze polovina antény. Výpočty nutné k návrhu jsem prováděla manuálně, potom pomocí simulačního programu CST MICROWAVE STUDIO a na závěr doladila výsledky v programu Smith.

Klíčová slova

RFID, biometrický pas, diferenciální anténa

Abstract

The first assignment was focused only on biometric passports and the construction of an RFID antenna for reading biometric passports. These are antennas in the high frequency band at a frequency of 13.56 MHz. During my studies, I found out that the issue is so broad and varied that it is not possible to separate only this part and focus only on it. These antennas are not manufactured by everyone, as they come with specialized software that must handle encryption, digital signature verification, etc. Combating passport counterfeiting requires that only certified and proven companies have access to these technologies. I could not provide a practical verification of the function of the antenna on a real device. That is why I had to test and tune the antenna on a commercially produced reader, which, despite all my efforts, I could not read either passport or ID card. I chose a relatively unusual antenna design - differential. It cannot be measured with a conventional spectrum analyzer because it has not two inputs and only half of the antenna had to be measured. I performed the calculations necessary for the design manually, then using the simulation program CST MICROWAVE STUDIO and finally fine-tuned the results in the Smith program.

Key words

RFID, biometric passport, differential antenna

Seznam použitých symbolů

Symbol	Jednotky	Význam symbolu
C_{pa}	F	Paralelní rezonanční kapacita
L_a	H	Výsledná indukčnost
L_0	H	Indukčnost v EMC filtru
P_{tot}	W	Celkový výkon
R_A	Ω	Odpor antény
R_Q	Ω	Sériový tlumící odpor
R_{match}	Ω	Výstupní odpor procesoru
R_{pa}	Ω	Paralelní tlumící odpor
R_{tr}	Ω	Reálná část Z_{tr}
S_{11}	Ω	Frekvenčně závislá vstupní impedance
T_i	S	Šířka impulsu
X_C	Ω	Kapacitní reaktance
X_L	Ω	Induktivní reaktance
X_{tr}	Ω	Imaginární část Z_{tr}
Z_{tr}	Ω	Transformovaná impedance
Z_0	Ω	Impedance
a_{avg}, b_{avg}	m	Střední rozměr vinutí
a_0, b_0	m	Vnější rozměry cívky
f_c	Bit/s	Přenosová rychlost
f_{r0}	Hz	Zlomová frekvence EMC filtru
ϵ_r	[-]	Relativní permitivita materiálu
Φ	Wb	Magnetický tok
B	Hz	Frekvenční šířka pásma
C	F	Kapacita
L	H	Indukčnost
M	[-]	Magnetická vazba

Na	z	Počet závitů
P	W	Elektrický výkon
Q	$[-]$	Jakost
R	Ω	Elektrický odpor
SWR	$[-]$	Koeficient impedančního přizpůsobení
d	m	Ekvivalentní průměr vodiče
f	Hz	Frekvence
g	m	Mezera mezi vedením
t	m	Tloušťka vedení
w	m	Šířka vedení
x	$[-]$	Mezivýpočet
α	dB/m	Útlum kabelu
λ	m	Vlnová délka
π	3,141592765	Ludolfovo číslo
ω	rad/s	Úhlová frekvence

Seznam použitých zkratek

Zkratka	Význam
PCD	Proximity coupling device (spojovací zařízení)
PICC	Proximity card (čipová karta s blízkou vazbou)
RF	Radio Frequency (radiofrekvenční)
RFID	Radio Frequency Identification (radiofrekvenční identifikace)
MRZ	Machine Readable Zone (strojově čitelná zóna)
NFC	Near Field Communication
BP	Bandpass (pásmová propust)
Carrier	Nosná
VF	Vysokofrekvenční
ID	Identification (identifikace)
M	Magnetická vazba dvou indukčností
K	Koeficient vzájemné vazby M
RFID tag	Jakékoliv zařízení se stejnou výbavou, jako PICC
EMC	Electromagnetic Compatibility
HLTB	Halt Command, Type B
REQB	Request command, type B (dotaz typu B)
WUPB	Wake up command, type B (dotaz po předchozím příkazu HLT)
ATQB	Answer to Request, Type B
ATTRIB	PICC selection command
N	Number of Anti-collision Slots
R	Random Number Selected by PICC during Anti-collision
PUPI	Pseudo Unique PICC Identifier
CRC	Cyclic Redundancy Check
CID	Card Identifier

Obsah

Úvod.....	- 14 -
1 RFID.....	- 15 -
1.1 Historie bezdrátové identifikace.....	- 15 -
1.2 Rozdělení podle frekvenčního pásma.....	- 16 -
1.3 Rozdělení podle způsobu napájení	- 17 -
1.4 Smyčkové antény pro pásmo HF.....	- 17 -
1.5 Princip přenosu elektrické energie prostorem	- 19 -
1.5.1 Počátky bezdrátového přenosu	- 19 -
1.5.2 Blízké a vzdálené pole.....	- 19 -
1.5.3 Napájení pasivního RFID čipu	- 20 -
1.6 Pasivní modulace signálu v RFID tagu	- 22 -
1.7 Nová karta v RF poli – komunikace na nejnižší vrstvě.....	- 29 -
2 Biometrický pas.....	- 31 -
2.1 Algoritmus čtení cestovního pasu	- 31 -
2.2 Bezpečnost dat.....	- 32 -
3 Návrh nové antény	- 34 -
3.1 Výpočet indukčnosti.....	- 35 -
3.2 Výpočet indukčnosti v CST Studiu	- 37 -
3.3 Simulace v programu Smith v4.1	- 44 -
4 Souhrn výsledků simulace.....	- 48 -
5 Testovací zdroj RFID signálu	- 52 -
6 Praktická realizace antény	- 55 -
6.1 Verifikace výsledků.....	- 58 -
6.1.1 První měření	- 59 -
6.1.2 Druhé měření.....	- 61 -
6.2 Návrh kompenzace antény	- 67 -
Závěr	- 70 -
Použitá literatura	- 71 -

Seznam příloh.....	- 74 -
--------------------	--------

Seznam ilustrací

<i>Obrázek 1.1: Frekvenční spektrum s používanými kmitočty[17].</i>	<i>- 16 -</i>
<i>Obrázek 1.2: Magnetická smyčková anténa[11].</i>	<i>- 18 -</i>
<i>Obrázek 1.3: Nikola Tesla při experimentu bezdrátového přenosu elektrické energie[15].</i>	<i>- 19 -</i>
<i>Obrázek 1.4: Vázané rezonanční obvody[12].</i>	<i>- 20 -</i>
<i>Obrázek 1.5: Přenos energie do RFID tagu [2].</i>	<i>- 21 -</i>
<i>Obrázek 1.6: Rozložení magnetického pole čtečky [2].</i>	<i>- 22 -</i>
<i>Obrázek 1.7: Průběhy při modulaci ASK z tagu v klasickém režimu [1].</i>	<i>- 23 -</i>
<i>Obrázek 1.8: Princip modulace a přenosu signálu z RFID tagu pomocí subnosné [2].</i>	<i>- 23 -</i>
<i>Obrázek 1.9: ASK spektrum a diodový demodulátor [2].</i>	<i>- 24 -</i>
<i>Obrázek 1.10: Rozprostření postranních pásem [2].</i>	<i>- 25 -</i>
<i>Obrázek 1.11: Vliv jakosti antény Q na příjem subnosných frekvencí [2].</i>	<i>- 25 -</i>
<i>Obrázek 1.12: Vliv rozladění antény RFID tagu na poměr úrovní subnosných frekvencí. Toto je konkrétní případ pro naši subnosnou 847 kHz používanou v biometrických dokladech [2].</i>	<i>- 26 -</i>
<i>Obrázek 1.13: Použití subnosných frekvencí ve vztahu k přenosové rychlosti [2].</i>	<i>- 26 -</i>
<i>Obrázek 1.14: Možné zapojení modulátoru v RFID tagu subnosnou frekvencí [2].</i>	<i>- 27 -</i>
<i>Obrázek 1.15: Vznik subnosné dvojí amplitudovou modulací [2].</i>	<i>- 28 -</i>
<i>Obrázek 1.16: Možné tvary signálů dle ISO/IEC 14443-2 [1].</i>	<i>- 29 -</i>
<i>Obrázek 1.17: Znázornění komunikace na více vrstvách.</i>	<i>- 30 -</i>
<i>Obrázek 2.1: Symbol biometrického pasu.</i>	<i>- 31 -</i>
<i>Obrázek 2.2: Ochranný obal proti nechtěnému přečtení[14].</i>	<i>- 32 -</i>
<i>Obrázek 2.3: Složení biometrického pasu[13].</i>	<i>- 33 -</i>
<i>Obrázek 3.1: Obecné připojení RFID antény k vysílači [2].</i>	<i>- 34 -</i>
<i>Obrázek 3.2: Nejčastější topologie impedančního přizpůsobovacího obvodu [3].</i>	<i>- 35 -</i>
<i>Obrázek 3.3: Reálné vlastnosti planární cívky.</i>	<i>- 35 -</i>
<i>Obrázek 3.4: Typická planární obdélníková anténa [4].</i>	<i>- 36 -</i>
<i>Obrázek 3.5: 3D model antény.</i>	<i>- 38 -</i>
<i>Obrázek 3.6: S_{11} parametry planární cívky.</i>	<i>- 38 -</i>
<i>Obrázek 3.7: Modulace ASK při přenosu typu A ISO14443.</i>	<i>- 39 -</i>
<i>Obrázek 3.8: Schéma zapojení pro snížení Q_a [4].</i>	<i>- 39 -</i>
<i>Obrázek 3.9: Převod na paralelní tlumící odpor [4].</i>	<i>- 40 -</i>
<i>Obrázek 3.10: Propojení vysílače – anténa a jejich přizpůsobení [4].</i>	<i>- 41 -</i>
<i>Obrázek 3.11: Transformace hodnot součástek mezi diferenciální a sigle anténou [3].</i>	<i>- 43 -</i>
<i>Obrázek 3.12: Vykompenzovaná anténa [4].</i>	<i>- 43 -</i>
<i>Obrázek 3.13: Doladování prvků pomocí Smithova diagramu (nepřesné doladění).</i>	<i>- 45 -</i>
<i>Obrázek 3.14: Změna přizpůsobení na 50 Ω.</i>	<i>- 47 -</i>
<i>Obrázek 4.1: Správně doladěná anténa k modulu vysílače.</i>	<i>- 49 -</i>
<i>Obrázek 4.2: Magnetická vyzařovací charakteristika vzdáleného pole.</i>	<i>- 49 -</i>
<i>Obrázek 4.3: Rozložení a intenzita magnetického pole na samotném substrátu.</i>	<i>- 50 -</i>
<i>Obrázek 4.4: Propad MP ve středu antény – detail.</i>	<i>- 50 -</i>

<i>Obrázek 4.5: Vyzařovací charakteristika v obou bokorysech je shodná.....</i>	<i>- 51 -</i>
<i>Obrázek 5.1: Dvojčinné zapojení anténní části modulu PN532 V3-1.....</i>	<i>- 52 -</i>
<i>Obrázek 5.2: HW úprava modulu PN532 V3_1.....</i>	<i>- 53 -</i>
<i>Obrázek 5.3: Pozlacené SMA konektory 50 Ω použité k propojení antény.....</i>	<i>- 54 -</i>
<i>Obrázek 5.4: Propojení Arduino_RFID modul_RFID anténa.</i>	<i>- 54 -</i>
<i>Obrázek 6.1: Schéma RFID antény pro čtení biometrických pasů.</i>	<i>- 55 -</i>
<i>Obrázek 6.2: Ladění antény na "dosah" a improvizovaný detektor EM pole.</i>	<i>- 56 -</i>
<i>Obrázek 6.3: Paměťová struktura karet MIFARE.</i>	<i>- 57 -</i>
<i>Obrázek 6.4: Začlenění ID.....</i>	<i>- 58 -</i>
<i>Obrázek 6.5: Porovnání zapojení dvou antén.</i>	<i>- 58 -</i>
<i>Obrázek 6.6: Závislost modulu Z na frekvenci.....</i>	<i>- 59 -</i>
<i>Obrázek 6.7: Detail Z v okolí paralelní rezonance.</i>	<i>- 60 -</i>
<i>Obrázek 6.8: Detail Z v okolí sériová rezonance.....</i>	<i>- 60 -</i>
<i>Obrázek 6.9: Závislost fáze na frekvenci.....</i>	<i>- 61 -</i>
<i>Obrázek 6.10: Měření rezonance.</i>	<i>- 62 -</i>
<i>Obrázek 6.11: Širokospektrální měření pouze planární indukčnosti s tlumícími odpory 14,6 Ω ve Smithově zobrazení.....</i>	<i>- 62 -</i>
<i>Obrázek 6.12: Široké spektrum k odhalení vlastních parazitních rezonancí.</i>	<i>- 63 -</i>
<i>Obrázek 6.13: Širší oblast spektra s laděnou a parazitní rezonancí zároveň.....</i>	<i>- 64 -</i>
<i>Obrázek 6.14: Zvětšený detail rezonanční křivky 13,56 MHz.....</i>	<i>- 65 -</i>
<i>Obrázek 6.15: Naměřená S11 charakteristika samotné antény ve Smithově zobrazení (zapojen pouze jeden vstup diferenciální antény, druhý je nezatížený). K měření byl použit koaxiální kabel 50 Ω délky 200 mm.</i>	<i>- 66 -</i>
<i>Obrázek 6.16: Simulovaná S11 charakteristika vystihující způsob měření, včetně měřícího kabelu.</i>	<i>- 67 -</i>
<i>Obrázek 6.17: Náprava posunuté impedance pomocí dvojice LC prvků.</i>	<i>- 67 -</i>
<i>Obrázek 6.18: Celkové upravené zapojení po korekci měřením.</i>	<i>- 68 -</i>
<i>Obrázek 6.19: Nové doladění na 50 Ω.....</i>	<i>- 68 -</i>
<i>Obrázek 6.20: Zapojení pouze vykompenzované antény na připojení ke čtečce 50 Ω.....</i>	<i>- 69 -</i>

Úvod

Tato práce je zaměřená na technologii RFID. Jedná se o radiofrekvenční identifikaci. Jak název napovídá, jedná se o komunikaci na základě bezdrátového přenosu informací za pomoci elektromagnetických vln.

Cílem práce je bližší seznámení s principem RFID komunikace. Tato komunikace může probíhat v blízkém poli (do 1 m), nebo ve vzdáleném poli (až do 15 m). Práce se zaměřuje hlavně na vysokofrekvenční obvody a parametry spojené s anténními systémy.

Dále je zde probrána problematika biometrických pasů, kam spadají antény se čtecím dosahem kolem 5 cm na kmitočtu 13,56 MHz. Tato anténa nachází využití nejen pro policejní kontroly, ale hlavně při automatickém odbavování cestujících. Biometrické pasy poskytují zvýšenou úroveň bezpečnosti dokladu samotného a snižují možnost jeho padělání či odcizení. Anténa samotná je jen prvním zařízením v řetězci na ní navazujícího bezpečnostního hardwaru a softwaru, který ale není součástí práce.

Prvotní záměr – sestrojím RFID anténu pro čtení biometrických cestovních dokladů, jsem měla na paměti až do jeho úplné realizace a myslím, že by v této podobě mohla být i používána.

Návrh antény je rozdělen do několika kroků. Nejprve je návrh prověřen výpočtem, poté nasimulován v programu CST MICROWAVE STUDIO a na závěr doladění jednotlivých součástek programem Smith.

Protože jsem ale potřebovala mít doma vlastní zařízení, na kterém bych mohla anténu testovat, zakoupila jsem modul k Arduino, který měl integrovanou anténu. Po jejím odpojení jsem ale nezískala potřebný kompatibilní výstup 50 Ω . Proto jsem zvolila metodu návrhu dvou variant antény. První anténa, aby pracovala se zakoupeným modulem a druhou anténu pomocí jednoduchého výpočtu doladit na 50 Ω .

Toto přizpůsobení jsem ověřovala laboratorním měřením i výpočtem, ale reálnou datovou komunikaci bylo možné ověřit pouze s podobnou PICC kartou typu MIFARE Classic. Ke komunikaci s cestovním pasem je nutný speciální software, který by s kartou komunikoval šifrovaně, pomocí klíče přečteného z optické, strojově čitelné zóny.

Bezkontaktní karty jsou rizikové, protože můžou být lehce přečteny i na větší vzdálenost a je tu velké riziko jejich zneužití. Je vhodné, aby se RFID karty a doklady nosili v elektricky vodivém pouzdře.

1 RFID

Radiofrekvenční identifikace je moderní technologie identifikace objektů za pomoci rádiových vln. Základní komponenty RFID jsou tag, anténa a čtečka. Využívají se různé frekvence, v závislosti na účelu použití. Frekvence má vliv na dosah, rychlost čtení a zápisu, hloubku pronikání materiálu, nebo elektromagnetickou kompatibilitu s okolním prostředím.

1.1 Historie bezdrátové identifikace

[20] Vývoj bezkontaktních RFID klíčů probíhá přibližně od konce II. světové války, a to hlavně pro vojenské účely. První systémy fungovaly například tak, že obsahovaly rezonanční obvod, který byl naladěn na nějakou harmonickou frekvenci vzhledem k té nosné, kterou vysílala čtečka. Přítomnost jiné frekvence byla za pomoci dalších filtrů detekována a tím došlo k potvrzení autentizace. Z dnešního pohledu to byly jedno-bitové RFID systémy.

S vývojem integrovaných obvodů došlo k tomu, že byly vytvořeny n-bitové systémy, které dokázaly přenést dostatečně dlouhý digitální autentizační klíč. Tyto tagy ve formě čipových karet, přívěšků, prstenů atd. se používají dodnes. Souží třeba jako náhrada klíčů, zjednodušení či omezení pohybu po budovách, nebo odstranily nutnost ručně vypisovat osobní kód na klávesnici bezpečnostního zařízení. Nevýhodou je, že se tagy dnes dají jednoduše klonovat a jejich majitel ztrácí nad bezpečností výhradní kontrolu. Původní představa byla taková, že se budou tagy vyrábět pouze v továrně a jejich ID bude jedinečné a neměnné. V současnosti se ID používá spíše jen jako softwarová antikolizní ochrana, když se do pole čtečky dostane více tagů současně.

V roce 1999 byl mezinárodní organizací pro civilní letectví ICAO vydán standart ISO/IEC 14443 pro RFID, skládá se ze 4 částí – fyzikální charakteristiky, radiofrekvenční výkonové rozhraní a signálové rozhraní, inicializace a antikolize, protokol přenosu. Kolem roku 2000 byly vyvinuty mikroprocesory, které mají ultra-nízkou spotřebu. Ty mohou v tagu on-line provádět množství důležitých operací, jako je šifrování přenášených dat, odstraňování kolizních situací s jinými tagy anebo aktualizace uložených dat. Při komunikaci se začaly používat standardní síťové protokoly. Tím se začala měnit i filozofie původního určení, a to je identifikace.

Vznikl systém NFC (Near Field Communication) pro komunikaci na blízkou vzdálenost. Zpočátku využívaný pro sdílení kontaktů a URL, přes bezpečné ukládání důležitých dat a digitálních klíčů až po platby. Na té nejnižší vrstvě jsou však oba systémy shodné, včetně nosné frekvence 13,56 MHz, která se používá na celém světě. Pro systém NFC však již vznikly nové standardy kvůli kompatibilitě mezi výrobci.

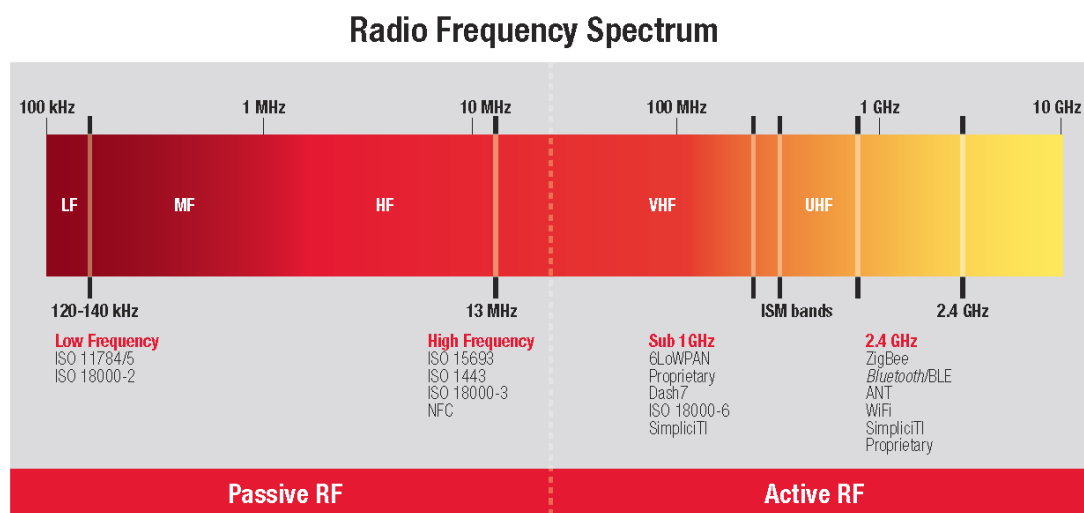
Mikročipy určené pro tagy, například platební karty, které doposud používaly pouze kontaktní čipy, tak byly zbaveny této nevýhody a byly povýšeny na bezkontaktní (resp. multifunkční). Stouplo ale zase bezpečnostní riziko odposlechu přenášených dat. Kromě jiného teď banky musí sledovat vzorce našeho chování a pokud počítač v bance zjistí nějakou

odchylku od našeho běžného chování, tak požaduje vložit do čtečky přímo kontaktní čip, zadat PIN, nebo je transakce zamítnuta úplně.

Většina výrobců mobilních telefonů NFC technologii montuje přímo do svých zařízení. Telefony tak mohou v těsném kontaktu sdílet data. Protože tato technologie funguje jen do vzdálenosti 4 cm, považuje se přenos za bezpečný a nešifruje se. Bohužel, pokud oba telefony fungují jako aktivní tagy, dá se jejich obousměrná komunikace zachytit až do vzdálenosti přibližně 10 m. Mezi další funkce telefonů patří i samotná možnost klonování pasivních RFID tagů, takže nemusíte nosit všechny karty s sebou.

1.2 Rozdělení podle frekvenčního pásma

Ve světě neexistuje úplně jednotná standardizace komunikačních frekvencí. Použitá frekvence má vliv na komunikační dosah, přenosovou rychlost, velikost antény i tagu, důležitý je i vliv okolí (kov, voda...) a interference ovlivňující úroveň signálu. Nižší frekvence znamená kratší dosah, pomalejší přenosovou rychlost a menší vliv okolí a naopak.



Obrázek 1.1: Frekvenční spektrum s používanými kmitočty[17].

- **Nízkofrekvenční – LF** (124 a 135 kHz) – vyznačují se velmi krátkým dosahem (jen několik cm) a nízkou přenosovou rychlostí. Na rozdíl od ostatních pásem ale vlny dobře pronikají kapalinou. Jako vysílací i přijímací anténu používají pouze z drátu navinutou cívku – smyčkovou anténu. Proto se dobře hodí například pro čipování zvířat, ale také do jednoduchých identifikačních karet.
- **Vysokofrekvenční – HF** (13,56 MHz) – mají přiměřený dosah (až 1 m), RFID tagy jsou schopné se napájet pouze z přenesené energie, mají větší přenosovou rychlost. Jako anténa se používá jen několik závitů drátu plošné cívky, která tak může být zhotovena fotocestou na plošném spoji nebo i na flexibilní ohebné podložce, čímž se zlevňuje proces výroby při jejich replikaci. Používají se hlavně k identifikaci zboží

v obchodech a též ve složitějších identifikačních kartách, které tak mohou využívat i kryptovaný přenos dat – viz cestovní pasy.

- **Ultra vysoké frekvence – UHF** (860 až 930 MHz) – mají větší dosah (až několik m), vysokou přenosovou rychlost, veškeré informace mohou být uloženy jen v RFID tagu. Nevýhodou je snižování dosahu přítomností vodivých materiálů v blízkosti antény. Také přesné frekvence nejsou na celé Zemi stejné, ale liší se podle kontinentů dle mezinárodních dohod. Přenášený výkon je však již tak malý, že RFID tagy musí mít vlastní zdroj energie, což se týká i mikrovln. Jako antény se používají tzv. meandrové antény, což jsou dipóly stočené do různých tvarů, aby se zachovala původní elektrická délka dipólu, ale aby se zmenšil celkový rozměr antény. Také se dají hromadně replikovat leptáním na plošném spoji nebo na ohebné podložce.
- **Mikrovlnná pásma – Microwave** (jednotky GHz) – používají se například na mytých branách na dálnici nebo při identifikaci zboží v letecké dopravě. Jako antény se také používají meandrové tvary.

1.3 Rozdělení podle způsobu napájení

- **Aktivní** – má vlastní zdroj energie, je stále zapnutý (neustále vysílá do okolí) a jeho komunikační dosah je mnohonásobně větší. Nevýhodou je omezená životnost každé baterie.
- **Semiaktivní** – má vlastní zdroj energie (vyšší dosah), ale aktivuje se až v okamžiku ozáření čtečkou. Tím se dosahuje prodloužení života baterie, ale za cenu pomalejší odezvy.
- **Pasivní** – používá výhradně energii přenesenou prostorem od čtecího zařízení. Do okamžiku ozáření tagu čtečkou je čip neaktivní.

1.4 Smyčkové antény pro pásmo HF

[11] Ke komunikaci mezi čtečkou PCD a PICC kartou se používá tzv. laděná smyčková (loop) anténa. Smyčkové antény se používají pro svou jednoduchost, nízké výrobní náklady a jejich všestranné použití. Mohou mít různé tvary: kruhové, trojúhelníkové, čtvercové, eliptické atd. Často se používají v telekomunikačních pojítcích dokonce až do mikrovlnných pásem cca 3 GHz. Používají se také jako elektromagnetické sondy. Protože byla vědecky potvrzena interakce RF magnetického pole s biologickými systémy, začala se tato anténa také používat pro magnetoterapii s různými frekvencemi. Jedná se o nechemickou a neinvazivní formu léčby, přičemž zatím nebyly zjištěny zásadní negativní vedlejší účinky tohoto VF elektromagnetického pole. Malé smyčky se používají jako kompaktní vysílací a přijímací antény v pásmu od 3 MHz do 30 MHz (nebo vlnové délky od 10 do 100 m).

V principu se jedná se o vodič stočený do cívky, která je buzena elektrickým proudem. Tím v jejím okolí vzniká střídavé VF magnetické pole. Vzhledem k této konstrukci je ale výrazně potlačeno pole elektrické. Protože v běžném prostředí vzniká množství průmyslového

rušení (napětíové špičky od motorů nebo spínaných zdrojů), jsou tyto antény velice výhodné, protože jsou na elektrické pole málo citlivé. Pracují hlavně s magnetickým polem.

Tak, jako má vertikálně postavená klasická drátová anténa všesměrovou vyzařovací charakteristiku tvaru „pneumatiky“, tak i smyčková anténa s vertikálně postavenou osou má charakteristiku stejnou. Rozdíl je pouze v tom, že pro zvyšování výkonu drátové antény je třeba zvyšovat napětí, zatím co u smyčkové proud. Specifickým případem je tzv. magnetická smyčková anténa (MLA – Magnetic Loop Antenna). Tu totiž tvoří vinutí několika málo závitů (postačuje i jeden závit) z měděné trubky. Tento závit může být například součástí feritového proudového transformátoru a tato trubka tvoří závit nakrátko.

Při vysílání tak může tímto závitem protékat proud desítky až stovky A. Podmínkou jakosti takové antény je tedy hlavně minimální odpor, což měděná trubka splňuje. Protože ale při takových frekvencích dochází také ke skin efektu, není vůbec nutné, aby měděná tyč byla plná, jelikož se proud šíří hlavně po jejím povrchu. Vyhovuje tedy tenkostěnná trubka, nejlépe s postříbeným povrchem.



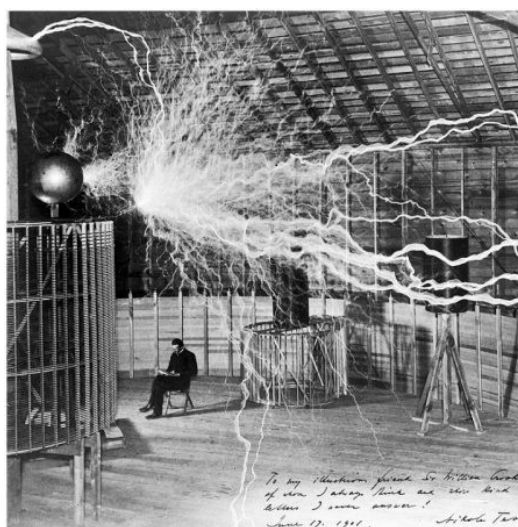
Obrázek 1.2: Magnetická smyčková anténa[11].

Další výhodou smyčkové antény, je právě vznik silného magnetického pole v blízkosti vinutí, takže může sloužit přímo jako VF transformátor elektrické energie pro napájení komunikačního čipu. Při modelování různých tvarů antén můžeme částečně ovlivnit výsledný tvar magnetického pole.

1.5 Princip přenosu elektrické energie prostorem

1.5.1 Počátky bezdrátového přenosu

Bezdrátový způsob přenosu elektrické energie, který vyvíjel světoznámý vynálezce Nikola Tesla, bohužel nefunguje tak, jak si to on představoval. Tesla byl průkopníkem využití střídavého proudu. K jeho výrobě používal rotační přerušovač, kterým dokázal vyrobit frekvence v řádu jednotek kHz. Tím napájel svůj VN transformátor, který stále zdokonaloval, a hlavně zvyšoval sekundární napětí. Zároveň k tomuto účelu stavěl vysoké věže se speciálním zářičem na vrcholu a předpokládal, že po dosažení toho „správného napětí“ obklopí celou Zeměkouli elektrickým polem, ze kterého bude možné čerpat energii kdekoliv na světě.



Obrázek 1.3: Nikola Tesla při experimentu bezdrátového přenosu elektrické energie[15].

Pomocí rádiových elektromagnetických vln se samozřejmě nějaká energie vždy přenáší od vysílače až k přijímači, ale s tak malou efektivitou, že se nevyplatí tento jev využívat jinak než pouze ke komunikaci.

1.5.2 Blízké a vzdálené pole

[19][22]Elektromagnetické pole okolo každé antény se rozděluje na tzv. „blízké pole“, kde převládá magnetická složka vlny a prakticky cokoliv, co se do této oblasti přiblíží, si nějakou energii odebere. V blízkém poli vznikají tzv. kvazistacionární vlny. Toto pole pozvolna přechází ve „vzdálené pole“, kde se elektromagnetická vlna odděluje od antény a začíná se šířit do volného prostoru jako rovinná vlna. Zde je poměr mezi elektrickou a magnetickou složkou již konstantní. Přesné rozhraní nelze přesně určit. RFID zařízení se také dělí na systémy blízkého pole (near field communication), které dokážou využívat energii vysílače i ke své vlastní spotřebě a na systémy vzdáleného pole, které musí mít vlastní zdroj energie.

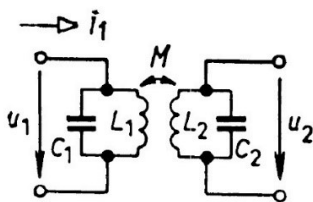
Přibližná vzdálenost tohoto rozhraní pro rozměry antén mnohonásobně menšími jako vlnová délka λ , se určí ze vztahu $r = \frac{\lambda}{2\pi}$. Jestliže $\lambda = \frac{c}{f} = \frac{3 \cdot 10^8}{13560000} = 22 \text{ m}$, potom $r \cong 3,5 \text{ m}$. To je teoreticky nejzazší mez, na kterou je možné komunikovat při dané frekvenci 13,56 MHz s pasivním RFID tagem (napájeným energií z elektromagnetického pole). Avšak všeobecně se uznává hodnota komunikace maximálně na 1 m.

Pokud do prostoru blízkého pole umístíme druhou anténu, vytvoří se mezi nimi vazba pomocí magnetické indukce. Tohoto principu se využívá také u transformátorů. Energie se tímto způsobem přenáší s daleko vyšší účinností.

Mikročipy, kterými jsou vybaveny RFID tagy, mají tak nízkou spotřebu energie, že se vyplatí je na několik vteřin ozářit výkonem do 2 W, jak stanovují limity ISO norem. Přitom přenos energie je poměrně jednoduchý a neškodný. Nyní podrobně popíšu funkci pasivního RFID tagu v pásmu HF.

1.5.3 Napájení pasivního RFID čipu

[12] Jak vysílací, tak i přijímací smyčkové antény mají naprosto shodné parametry. Zdůrazňuji, že se jedná o dva paralelní rezonanční obvody (PRO) s magnetickou vazbou (Obrázek 1.4). PRO pracuje tak, že pokud na jeho svorky přivedeme střídavé napětí o stejné frekvenci, jako je jeho rezonanční frekvence $f_0 = \frac{1}{2\pi\sqrt{L \cdot C}}$, začne tento obvod rezonovat tím způsobem, že se mezi kapacitou a indukčností začne střídavě přelévát značné množství energie ve formě střídavého elektrického proudu. Tento proud je mnohem větší, jako je proud dodávaný ze zdroje signálu. Čím větší je jakost rezonančního obvodu Q , tím větší proud I_r uvnitř obvodu protéká. Tento rezonanční proud protékající indukčností vyvolává v jejím okolí také Q krát vyšší magnetický tok Φ v porovnání se situací, kdy by nebyl paralelně připojený rezonanční kondenzátor C , resp. kdyby PRO nebyl v rezonanci.

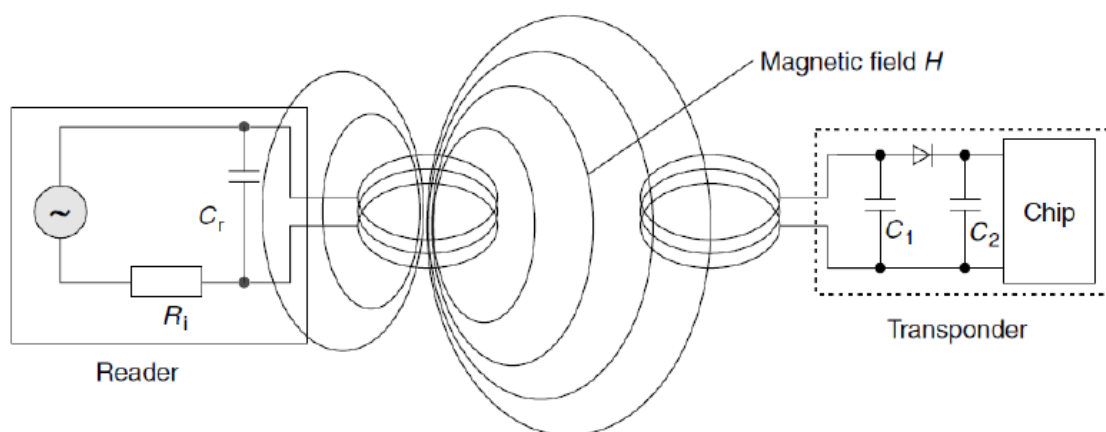


Obrázek 1.4: Vázané rezonanční obvody[12].

Když tedy do tohoto střídavého magnetického pole o frekvenci f_0 vložíme druhý PRO naladěný na stejnou frekvenci, začne tento sekundární obvod také rezonovat, protože bude buzen tímto polem přes indukčnost L .

Co se nám tedy stane přiblížením těchto dvou PRO do těsné blízkosti se silnou magnetickou vazbou M ? Celý systém se přemění na vysokofrekvenční transformátor. Názorné schéma napájení můžeme vidět na Obrázek 1.5. Vázané PRO jsou právě pro tuto svou vlastnost

využívány k poměrně efektivnímu bezdrátovému přenosu elektrické energie (například bezdrátové nabíjení mobilního telefonu). Když k tomu druhému, sekundárnímu PRO připojíme zátěž, tak stoupne odběr proudu z generátoru dodávajícího energii do toho prvního, primárního vysílajícího PRO. R_i v zapojení readeru slouží právě k indikaci změny odběru proudu z vysílače. Úbytek napětí na tomto odporu je přímo úměrný odebíranému proudu. Když tedy budeme v transpondéru zvyšovat a snižovat zátěž (klíčováním z mikroprocesoru), můžeme tyto změny okamžitě snímat na odporu R_i . To je základní princip pasivního přenosu dat z transpondéru zpět k vysílači (čtečce). Velikost signálu pronikajícího z primárního obvodu do sekundárního, a naopak se posuzuje součinitelem vazby $k = \frac{M}{\sqrt{L_1 \cdot L_2}}$ kde M vyjadřuje vzájemnou magnetickou vazbu obou obvodů.



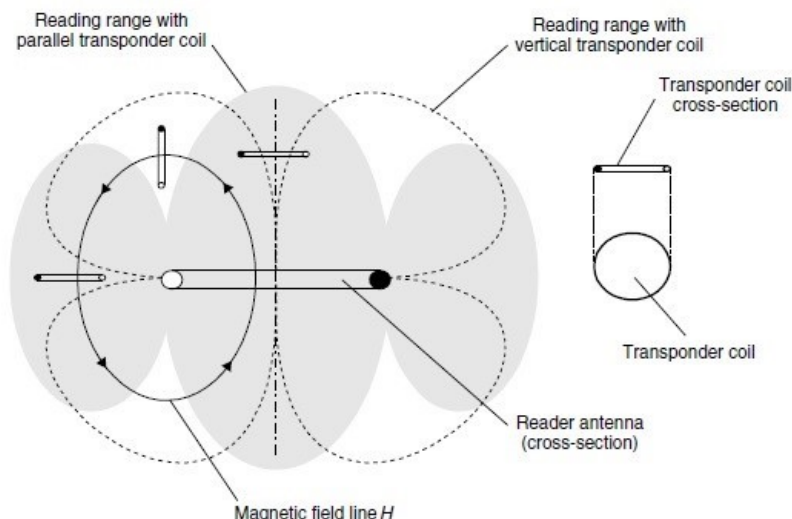
Obrázek 1.5: Přenos energie do RFID tagu [2].

Kapacita C_1 je rezonanční kapacitou s indukčností L vinutí přijímací smyčkové antény (PRO). C_2 je filtrační kapacitou napájecího napětí pro čip. Její minimální velikost závisí na reálném odběru energie čipem. C_2 má za úkol odstranit (odfiltrovat) všechny střídavé složky z napětí usměrněného předchozí diodou. Vzhledem k odběru čipu a frekvenci indukovaného napětí to budou odhadem jednotky až desítky nF.

Protože se ale jedná o vzduchové cívky různých velikostí a tvarů, bude nejsilnější magnetické pole hlavně v těsném okolí vodičů vinutí, a nikoliv v celém prostoru cívky. Čím efektivnější přenos energie tedy chceme, tím těsněji musíme přiblížit obvody vinutí cívek obou PRO. Z toho vyplývají hlavně závislosti na rozměrech obou cívek, které však podle účelu použití nemusí mít vždy stejné rozměry i když jejich rezonanční frekvence musí být stejné. Z hlediska vzájemného umístění obou cívek je však téměř úplně jedno, jestli budou mít stejné rozměry a budou od sebe vzdáleny např. 1 cm anebo jestli budou umístěny v jedné rovině a jejich rozměry se po celém obvodu budou o 1 cm lišit. Jedná se výhradně o vzájemné vzdálenosti vinutí u rozměrných cívek.

Když tedy pro elektronický pas vytvoříme smyčkovou anténu o několik cm větší, jako je anténa zalísovaná v ID kartě uvnitř, tak získáme určitý manipulační prostor s neměnnou

intenzitou magnetického pole, protože posunem pasu po ploše libovolným směrem se vždy jedna vzdálenost mezi vinutími zmenší a druhá zvětší.



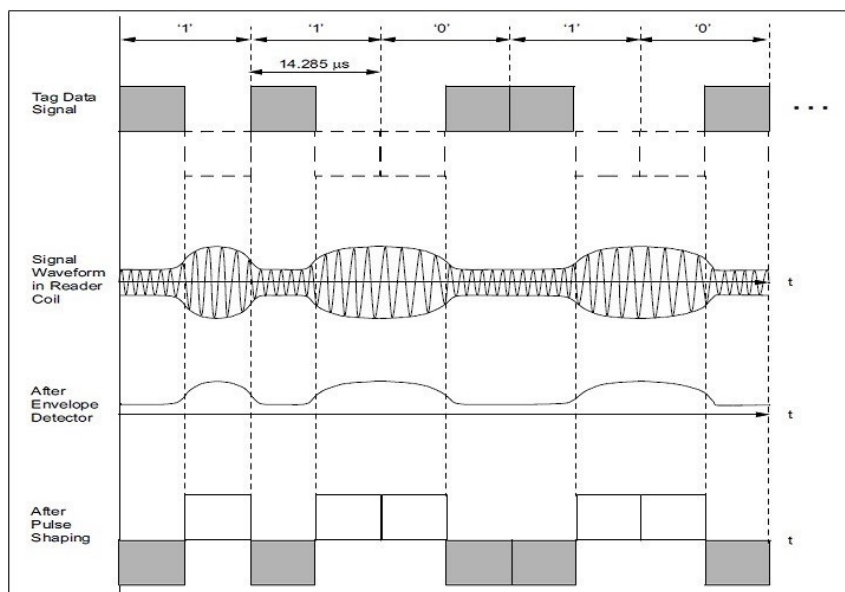
Obrázek 1.6: Rozložení magnetického pole čtečky [2].

Pro zvětšení manipulační plochy se dají také použít spirálové antény, které vykryjí celou vnitřní plochu, ale pro náš účel je tato plocha vyhrazena pro optickou čtečku strojově čitelné zóny. Naštěstí si světlo a magnetické pole v našich podmínkách nijak nevadí.

1.6 Pasivní modulace signálu v RFID tagu

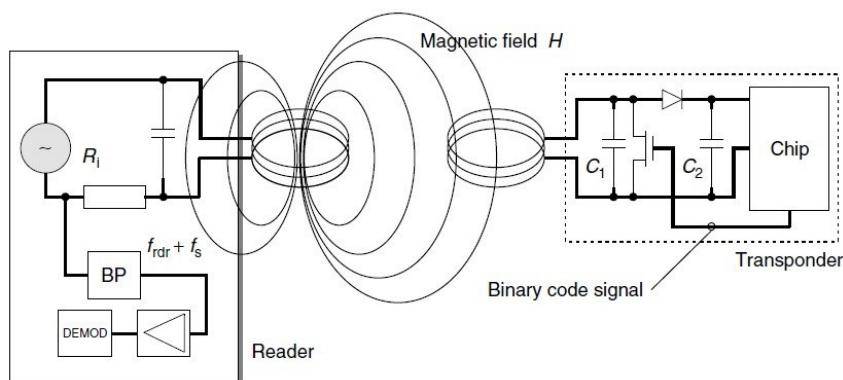
[2][1] Z výše uvedeného existuje několik způsobů, jak změnou některého z parametrů sekundárního PRO můžeme ovlivnit zatěžovací proud generátoru vysílaného, nosného signálu. Naším cílem je co nejvíce změnit proud vysílače, ale co nejméně narušit napájení čipu v RFID tagu a zároveň i dosah pro fungující komunikaci. Nejčastěji se používá tzv. zátěžová modulace. Ta funguje tak, že se k PRO antény tagu střídavě připojuje odpor s nízkou hodnotou, řádově několik Ω . Tím se skokově zvýší zatížení antény až na maximum. Odpor se připojuje pomocí tranzistoru, klíčováného mikroprocesorem. Dochází tak k amplitudové modulaci nosného signálu (ASK).

Se zátěžovou modulací jsou však spojeny další potíže. V důsledku slabé induktivní vazby M demodulované napětí na straně čtečky velice kolísá a je až o několik řádů menší, v porovnání s napájením vysílací antény. V praxi, kdy se na anténě RFID tagu 13,56 MHz v rezonanci indukuje napětí až 100 V, je užitečný signál v přijímači kolem 10 mV při odstupu signál/šum 80 dB. Detekce takto malých změn vyžaduje velice komplikované obvody, aby detekovaly blízká postranní pásma vzniklá amplitudovou modulací.



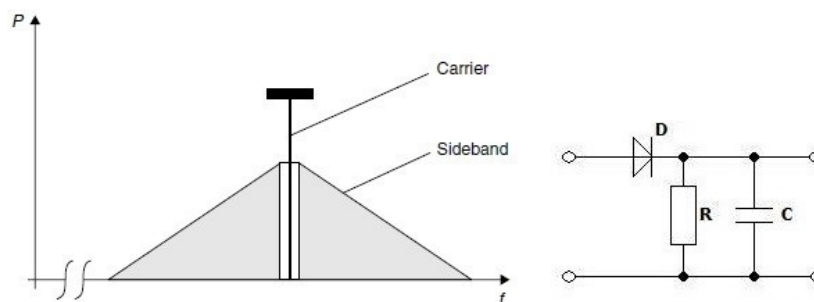
Obrázek 1.7: Průběhy při modulaci ASK z tagu v klasickém režimu [1].

Obrázek 1.8 zobrazuje princip komunikace pomocí subnosné frekvence ze směru od tagu ke čtečce. Data z tagu jsou přenášena na jiné (subnosné) frekvenci. V přijímači na straně čtečky kde se odfiltruje subnosná frekvence filtrem BP a dále je zpracována bez nosné frekvence.



Obrázek 1.8: Princip modulace a přenosu signálu z RFID tagu pomocí subnosné [2].

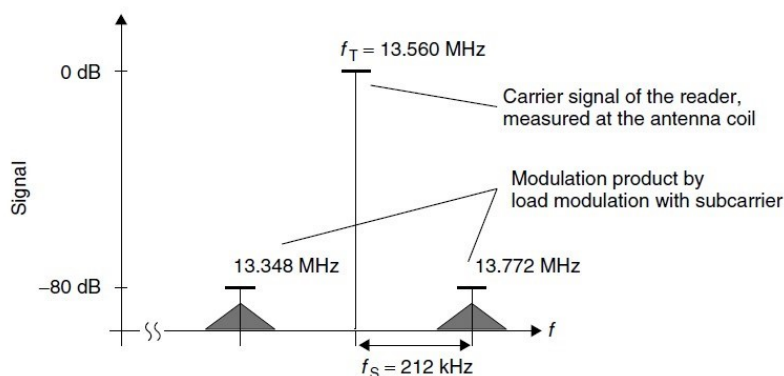
Samotná sinusová nosná vlna bez modulace je ve frekvenčním spektru pouze vyobrazena jako úzká čára, v našem případě o frekvenci 13,56 MHz. Když do modulátoru přivedeme jako modulační signál tok jedniček a nul s frekvencí 212 kHz, vzniknou nám další dvě postranní frekvence okolo té nosné a sice $f_n \pm f_p$. Ale protože tok dat jsou náhodně se vyskytující jedničky a nuly, je frekvence dat f_d vlastně funkcí šumu.



Obrázek 1.9: ASK spektrum a diodový demodulátor [2].

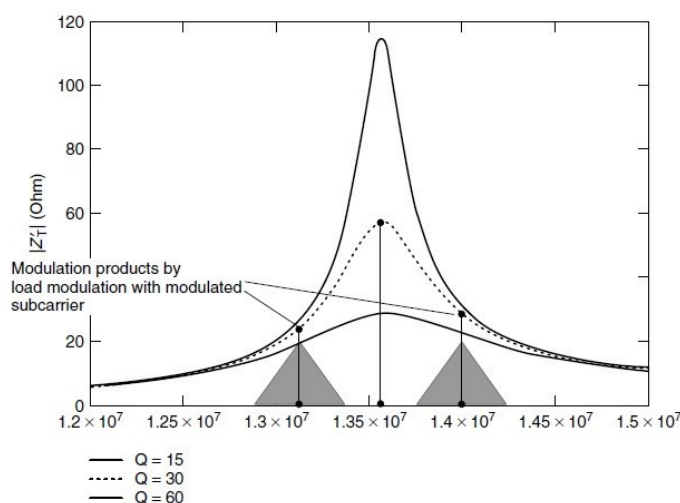
Nikdy se tedy nedá přesně určit modulační frekvence, a proto se postranní pásma ve frekvenčním spektru rozprostírají více do šířky, tak jak to ukazuje Obrázek 1.9. Přenos dat tedy není realizován nosnou frekvencí, ale pouze těmi postranními pásmy. K oddělení dat nám stačí pouze jedno z nich. Pokud je hloubka modulace, a tedy i úroveň postranních pásem dostatečná, stačí nám k demodulaci prostý diodový detektor (amplitudový demodulátor). Nejdůležitější je zde správná volba časové konstanty RC , protože tento obvod má za úkol odstranit nosnou frekvenci, ale propustit frekvenci modulační. Když je ale hloubka modulace velice nízká, tak jako je to u zátěžové modulace v tagu, užitečný signál se nám ztratí pod úroveň zvlnění vzniklého filtrací nosné vlny. Je to způsobeno právě tím, že jsou ve frekvenčním spektru tato postranní pásma příliš blízko k nosné vlně.

Proto se sama nabízí myšlenka, jak zvětšit frekvenční odstup postranních pásem? Hodiny v tagu jsou odvozeny pouze od frekvence nosného signálu. Kdybychom měli k dispozici patřičnou frekvenci a prováděli dvojí modulaci (tzn. že ještě před zátěžovou modulací vložíme druhý), tak nám vznikne spektrum trochu širší – viz Obrázek 1.10. Vzniknou nám dvě, vlastně samostatné nosné frekvence, které tu nosnou nepotřebují (samozřejmě nosná je zdroj energie). Na přijímací straně, tedy ve čtečce, se jedno z těchto pásem odfiltruje frekvenční propustí BP (bandpass), čímž se maximálně potlačí rušivý vliv samotné nosné. Modulaci subnosné frekvence lze provádět všemi druhy modulací (ASK, FSK i PSK). Subnosná 212 kHz je zde vybrána pouze jako příklad a používá se v systémech long-range s dosahem až 1 m. Norma ISO/IEC 14443-2 však uvádí jedinou subnosnou $f_s = 847$ kHz.



Obrázek 1.10: Rozprostření postranních pásem [2].

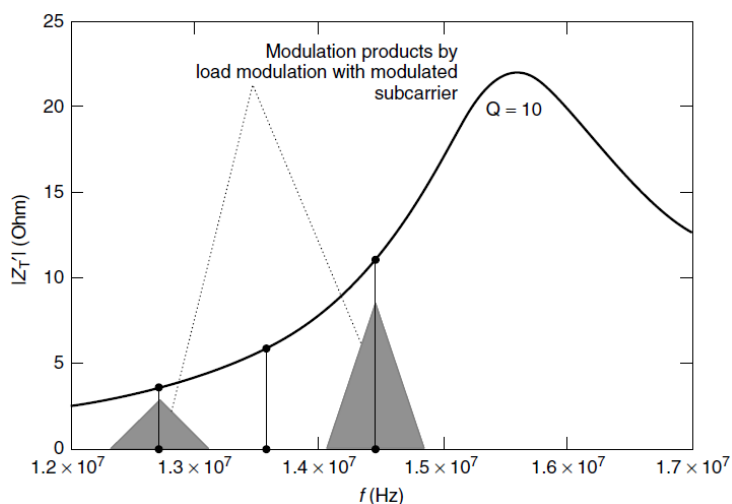
Využití postranních pásem se v informatice dnes běžně používá a u NFC technologií je upřednostňované. Určitým kompromisem pak musí být zvolená jakost RFID antény Q_a , protože obě antény musí přenést celou šířku pásma. Pokud by byla jakost příliš vysoká, zúžilo by celkové přenosové pásmo B a postranní pásma se subnosnými by byla zase potlačována. V praxi se používá $Q \leq 50$. Tímto způsobem se dosahuje vyšší přenosové rychlosti s RFID tagem, například u platebních karet, ale zase na úkor dosahu, který činí maximálně několik cm. Je to daň za snížení jakosti Q antény a tím i jejího zisku. Naopak v aplikacích, kde stačí přenést pouze ID (nízká přenosová rychlost), jako například klíčenky, raději použijeme přenos bez použití subnosné, zvýšíme Q_a , a můžeme snímat tagy například v identifikačních bránách v obchodech. Návrh správné jakosti Q_a , je vždy kompromisem mezi dosahem a přenosovou rychlostí.



Obrázek 1.11: Vliv jakosti antény Q na příjem subnosných frekvencí [2].

Současné RFID systémy, softwarově doplněné o antikolizní procedury, dokážou současně obsloužit až 15 karet v jednom EM poli. To však vyvolává další potíže se zátěžovou modulací, protože se karty vzájemně ovlivňují.[9]

Proto se některé karty pracující v systémech 13,56 MHz vybavené antikolizní procedurou úmyslně rozladí. Už při výrobě se rezonanční obvod antény naladí do pásma (15-18) MHz. Tím dojde k tomu, že už při odesílání dat z karty do čtečky jsou subnosné frekvence vysílány s jinou úrovní a vliv nosné je potlačen (Obrázek 1.12). Zároveň se tím omezuje vzájemné ovlivňování ostatními kartami.



Obrázek 1.12: Vliv rozladění antény RFID tagu na poměr úrovní subnosných frekvencí. Toto je konkrétní případ pro naši subnosnou 847 kHz používanou v biometrických dokladech [2].

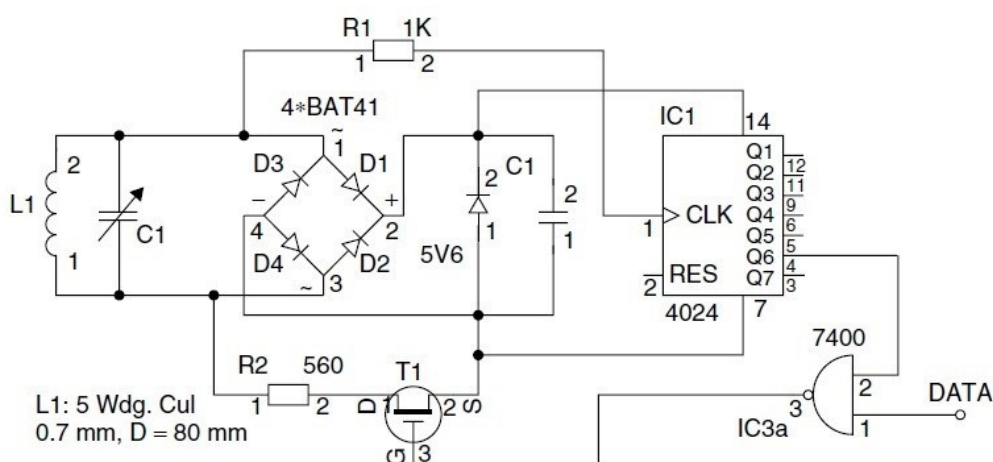
Na **Error! Reference source not found.** je tabulka se souhrnem nejčastěji používaných subnosných frekvencí v závislosti na přenosové rychlosti a dosahu.

System	Baud rate	$f_{\text{Subcarrier}}$	f_{TX}	Range
ISO 14443	106 kBd	847 kHz	13.56 MHz	0–10 cm
ISO 15693 short	26.48 kBd	484 kHz	13.56 MHz	0–30 cm
ISO 15693 long	6.62 kBd	484 kHz	13.56 MHz	0–70 cm
Long-range system	9.0 kBd	212 kHz	13.56 MHz	0–1 m
LF system	–0–10 kBd	No subcarrier	<125 kHz	0–1.5 m

Obrázek 1.13: Použití subnosných frekvencí ve vztahu k přenosové rychlosti [2].

Pomocí subnosné se provádí modulace v pasivním RFID tagu. V RFID čtečce se naopak využívá toho, že je zdrojem nosné frekvence a dokáže ji modulovat s hloubkou modulace 100 %, modulaci pomocí subnosné proto nepoužívá (pouze ji přijímá). Demodulace signálu v RFID tagu klasickým demodulátorem je tedy jednoduchou záležitostí.

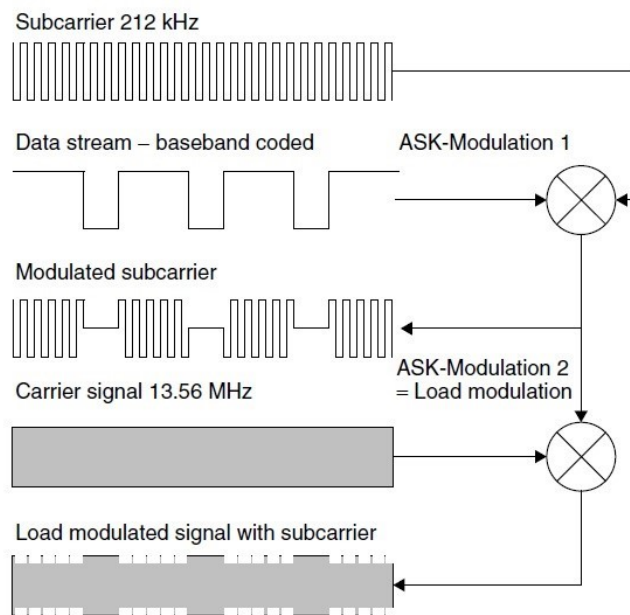
Na následujícím Obrázek 1.14 je navrženo jedno z možných zapojení modulátoru RFID tagu se subnosnou. Nosný signál (vysílaný RFID čtečkou) a přijímaný rezonanční anténou tagu L1, C1 je usměrněn můstkovým usměřovačem, filtrován kondenzátorem C1 a vzniklé stejnosměrné napětí je stabilizováno zenerovou diodou na 5,6 V. Tímto napětím jsou napájeny všechny elektronické obvody. Zároveň je z antény přes ochranný odpor R1 vedena nosná frekvence do hodinového vstupu IC1, což je 7bitový CMOS binární dělič 74HC4024. Z výstupu Q6 je odebírána frekvence subnosné, získaná vydělením frekvence nosné binárním děličem, tedy $f_s = 13,56 \text{ MHz} / 2^6 = 212 \text{ kHz}$. Subnosná je vedena spolu s daty do hradla NAND, kde dochází k 1. modulaci ASK-1. Výstup hradla spíná tranzistor T1, který k rezonanční anténě připojuje zatěžovací odpor R2 (proto se pro tuto metodu používá výraz „zatěžová modulace“). Prakticky se tímto odporem utlumí rezonanční kmity a stoupne odběr z vysílače RFID čtečky. T1, R2 nám vytváří modulátor ASK-2.



Obrázek 1.14: Možné zapojení modulátoru v RFID tagu subnosnou frekvencí [2].

Subnosná frekvence podle normy ISO/IEC 14443-2 vznikne vydělením nosné frekvence $13,560 \text{ MHz} / 16 = 847 \text{ kHz}$. Uvedené příklady se vztahují i k jiným subnosným z uvedené tabulky na **Error! Reference source not found.**

Na následujícím Obrázek 1.15 je graficky znázorněn vznik subnosné frekvence ve výše popsaném obvodu.

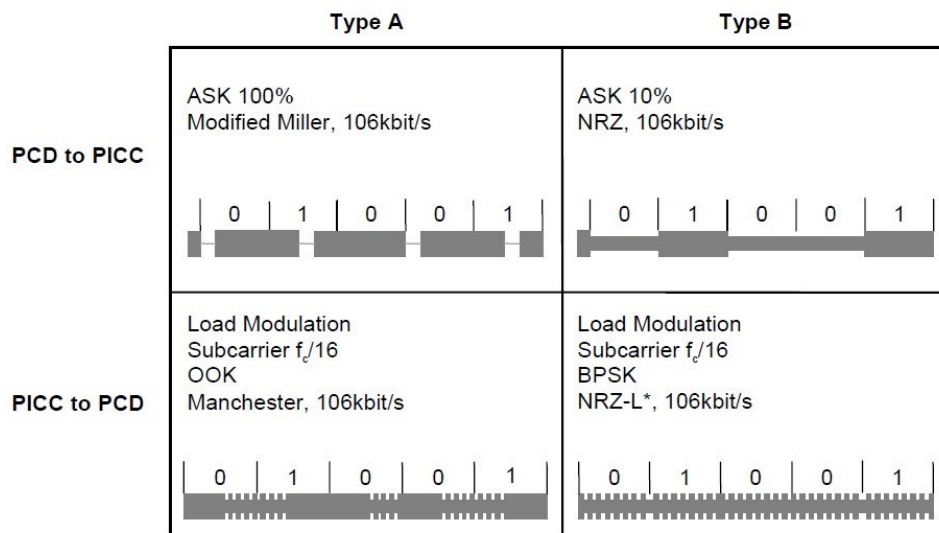


Obrázek 1.15: Vznik subnosné dvojí amplitudovou modulací [2].

Použití modulace subnosnou frekvencí má větší dosah a při přenosu vzniká méně chyb. Třicetiletý vývoj NFC technologií však zanechává také jisté následky. Každý výrobce používá jiné patenty a technologie. Proto to jediné, co je sjednocuje, jsou mezinárodní normy. Každý RFID tag byl někdy vyroben a požadujeme, aby do konce své životnosti pracoval, pokud možno se všemi čtečkami. Proto nejsložitějším zařízením je v současnosti RFID čtečka, která musí zabezpečit kompatibilitu napříč všemi verzemi RFID tagů.

Mezinárodní norma ISO/IEC 14443-2 definuje datový přenos z PCD (RFID čtečka) do PICC (karta pro komunikaci na krátkou vzdálenost) na nosné vlně $f_c = 13,56$ MHz, přenosovou rychlost $f_c = 13560 / 128 = 106$ kbit/s a amplitudovou modulaci ASK. Toto jsou hlavní společné parametry, protože se ještě rozdělují na typ A nebo typ B, lišící se pouze hloubkou modulace a metodou sériového přenosu.

Přenos zpět PICC – PCD bude prováděn pomocí subnosné frekvence odvozené dělením nosné $f_s = 13560 / 16 = 847$ kHz a přenosovou rychlostí opět 106 kbit/s. U typu A je subnosná modulovaná pouze amplitudově ASK. Typ B moduluje subnosnou fázově BPSK.



* Inversion of data is also possible

Obrázek 1.16: Možné tvary signálů dle ISO/IEC 14443-2 [1].

1.7 Nová karta v RF poli – komunikace na nejnižší vrstvě

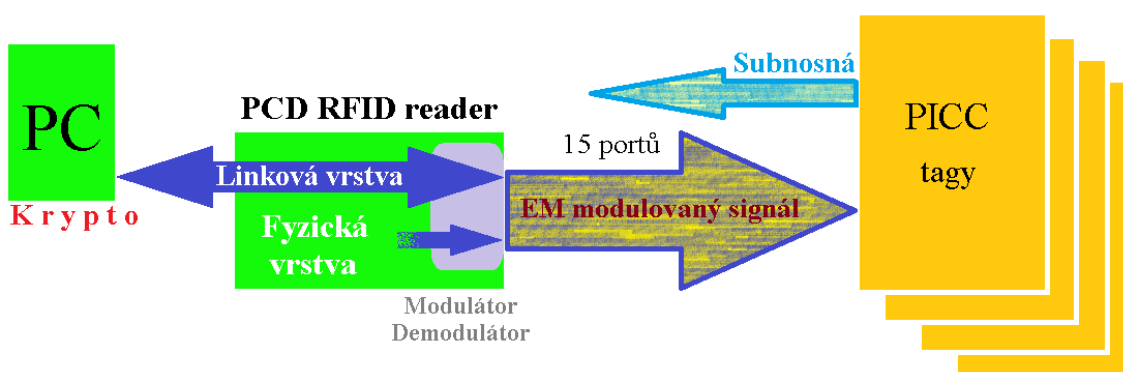
[9][10][6][24] Zde popisují postup PCD čtečky pro nastavení a zavedení nově přichází RFID karty (karet) do již existujícího RF pole. Tyto operace jsou součástí antikolizních procedur, přičemž čtečka o tom nepředává žádné informace, dokud karta nevstoupí do další komunikační vrstvy. Norma ISO14443 povoluje dva typy komunikace A a B. V tomto popisu se detailně věnuji typu „B“, ale není mezi nimi výraznějších rozdílů.

Nově aktivovaná karta v RF poli se restartuje a tiše čeká. RFID čtečka vysílá trvale nosnou vlnu 13,56 MHz a v pravidelných intervalech střídavě vysílá příkaz REQA a REQB (Request type A or B), aby ověřil přítomnost nového zařízení v elektromagnetickém poli. Součástí tohoto příkazu je také číslo N (Number of Anti-collision Slots), které udává předpokládaný počet slotů volných pro připojení ke čtečce. Je to součást antikolizní procedury (může jich být až 15). Pokud kterákoliv karta PICC přijme příkaz s $N = 1$, tak odpoví okamžitě. Subnosnou frekvenci zapíná až v okamžiku, když hodlá odeslat nějaká data. Její zapnutí a následné vypnutí však podléhá přesné specifikaci v ISO14443-3, aby se mohl nafázovat přijímač ve čtečce. Jakmile je ale PICC karet v poli více, začnou komunikovat současně a čtečka vyhodnotí chybný kontrolní součet CRC (Cyclic Redundancy Check). Z toho odvodí, že karta není sama a odešle další příkaz REQB, ale s vyšším N.

Všechny karty po obdržení tohoto příkazu ihned vygenerují náhodná čísla R (Random Number Selected by PICC during Anti-collision) v rozsahu 1 až N, čímž se trochu zvýší pravděpodobnost správného pořadí. Karta, která si vygenerovala $R = 1$ (může jich samozřejmě být i více), tak odpoví příkazem ATQB (Answer to Request, Type B) a do něho vloží PUPI (Pseudo Unique PICC Identifier), které se používá pro antikolizní řízení komunikace. PUPI je 4

– Bytové číslo, které může být dynamicky vygenerované nebo pevně naimplementované. Karty s $R > 1$ přejdou zpět do výchozího stavu a mlčí. Jestliže karta s $R = 1$ byla sama a úspěšně provedla přenos, tak jí čtečka odešle příkaz HLTB (HALT state and stop responding to a REQB), čímž ji uspí a dalšího procesu se už nebude zúčastňovat (nebude odpovídat na dotaz REQB). Pokud ale CRC nesouhlasí, budou všechny karty pokračovat na dotaz REQB stejnou, stále se opakující procedurou, až do splnění všech požadavků.

Karty, které byly uspané příkazem HLTB, se probudí až teprve příkazem WUPB (Wake up command type B). Následně čtečka pomocí příkazu ATTRIB (PICC selection command) přidělí každé PICC kartě vyhrazené číslo kanálu CID (Card Identifier) z rozsahu 0 až 14 a PICC tímto přejde do vyšší komunikační vrstvy. Teprve tehdy může podle potřeby PC s kartou zahájit šifrování datového přenosu, přičemž čtečka slouží již jen jako komunikační switch.



Obrázek 1.17: Znáznornění komunikace na více vrstvách.

2 Biometrický pas

[23][10] Každý biometrický pas má dva základní znaky:

- Stránka dokladu, na které jsou uvedeny osobní informace, je vyrobena z tuhého plastu.
- Na přední straně desek je mezinárodní symbol pro biometrický pas.



Obrázek 2.1: Symbol biometrického pasu.

Podle standartu ISO/IEC 14443 pro RFID, komunikační dialog mezi čtečkou PCD (Proximity Coupling Device) a PICC (Proximity Integrated Circuit Card) kartou by měl být induktivní. Napájení a komunikace musí probíhat skrz modulovaný RF signál. Pracovní frekvence bude $13,56 \text{ MHz} \pm 7 \text{ kHz}$. Ke komunikaci mohou být použity dva typy komunikačních metod, typu „A“ nebo „B“. Po detekci typu čipu již bude komunikace probíhat jen jednou z metod. Maximální výkon vysílače 2 W a maximální komunikační vzdálenost bude 10 cm.

2.1 Algoritmus čtení cestovního pasu

Z technického hlediska je postup komunikace s PICC kartou vždy stejný. Ověřování a zabezpečení dat uložených v čipu je SW záležitostí:

- Oskenování a přečtení údajů ve strojově čitelné zóně MRZ – Machine Readable Zone. Tato zóna se používá již od roku 1980. Jediným bezpečnostním prvkem je kontrolní kód.
- Na základě těchto přečtených údajů se vytvoří klíč pro šifrovaný přenos dat, bez kterého se s čipem nedá plně komunikovat.
- Spuštění nosné frekvence 13,56MHz a vyčkání minimální pauzy, kdy proběhne aktivace napájení komunikačního čipu v ověřovaném PICC dokladu, jeho restart a čekání na příjem amplitudově modulovaného dotazu.
- Protože dle výše uvedené normy ISO 14443 jsou povoleny dva možné způsoby komunikace, začne čtečka střídavě vysílat dotazy typu A a následně typu B.
- V okamžiku, kdy čtečka zachytí první odpověď, která obsahuje hlavně typ modulu a s tím spojený druh modulace, bude dále probíhat komunikace jen podle zvolené verze modulace a šifrováním odvozeným ze strojově čitelné zóny. Bez znalosti šifrovacího klíče z MRZ (Machine Readable Zone) komunikovat nebude.

2.2 Bezpečnost dat

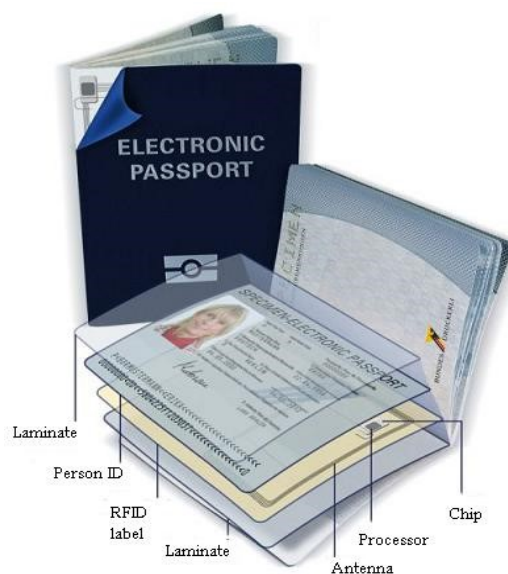
Protože cestovní pasy jsou v zájmu padělatelů a zlodějů, je nutné data nějak chránit. Nejslofistikovanějším způsobem krádeže dat je jejich přečtení přímo v kapse majitele. Když totiž zesílíme výkon RF signálu, lze s čipem navázat komunikaci i na větší vzdálenost. Proto je nutné nejprve získat fyzický přístup k dokladu a opsat strojově čitelné řádky. Čip tedy nebude odesílat žádná data, dokud neobdrží správný šifrovací klíč. Bohužel už to, že na úrovni základní komunikace na sebe čip prozradí svůj typ anebo pokud má jen statické PUPI (Pseudo Unique PICC Identifier), tak uvádí svého majitele do nebezpečí. Zloděj tím dokáže přesně lokalizovat jeho uložení a doklad odcizit. Majitelům biometrických cestovních dokladů je doporučeno nosit doklad v elektricky vodivém obalu, který zabrání průniku RF signálu a neprozradí se. Na obrázku 15 je vidět prodávané obaly s pokovenou vnitřní stranou. V nouzi ale stačí zabalit cestovní pas třeba do pozlátka od čokolády.



Obrázek 2.2: Ochranný obal proti nechtěnému přečtení[14].

Jelikož má klíč odvozený od údajů ze strojově čitelné zóny malou entropii a je statický, tak i v případě zachycení reálné komunikace se čtečkou je možné „hrubou silou“ klíč prolomit. Stejný problém se týká také „bezkontaktních kreditních karet“. Jednorázová platba do výše 500 Kč může v současné době proběhnout bez zadání PINu i bez vědomí svého majitele.

Proti krádeži a úpravě biometrických dat je čip chráněn úplným uzamčením. Po vydání pasu příslušným úřadem již nelze data měnit. Každý úřad, který je oprávněn vydávat tyto pasy, má také centrálně přidělený digitální podpis, kterým se údaje na čipu podepisují, aby bylo možné zpětně ověřit, že data nejsou změněna. Na čipu je též uložený nezbytný certifikát, který umožňuje tento podpis ověřit. Tento proces se nazývá „pasivní autentifikace“. Je to nejdůležitější mechanismus, který by měl odhalit padělání pasu. Na základě provedených kontrol však bylo zjištěno, že až 50 % terminálů propustilo pas s chybným digitálním podpisem od vydávajícího úřadu.



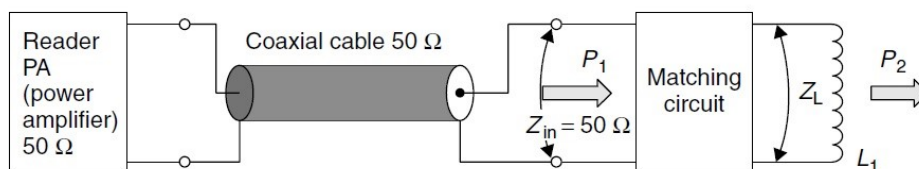
Obrázek 2.3: Složení biometrického pasu[13].

Karta obsahuje ještě další digitální klíč, určený pro tzv. „aktivní autentifikaci“. Klíč je rozdělen na dvě části, přičemž ta privátní je uložena v nepřístupné části paměti. Je to další mechanismus proti klonování dokladů. Při navázání komunikace se tímto podpisem podepisuje tzv. „challenge“, který zároveň může být použit jako důkaz, že dotyčná osoba v daný čas byla na určitém místě. Problém je ovšem v tom, že PICC čip nemá hodiny a datum mu může být podvrženo. Tento nedostatek řeší jiný mechanismus vyvinutý v Německu – EAC (Extended Access Control), fungujícím na protokolu Diffie-Hellman, pro výměnu klíčů. Tento mechanismus zároveň ověřuje důvěryhodnost samotného terminálu a na základě toho mu umožní číst citlivější údaje, jako je otisk prstu nebo sken duhovky.

3 Návrh nové antény

[3] Jelikož je každé RFID čtení biometrického pasu spojeno s jeho celoplošným optickým skenováním (kvůli strojově čitelné zóně), je asi bezpředmětné, zabývat se plošnou anténou se spirálovým vinutím. Taková anténa je vhodná pouze pro kreditní nebo jiné identifikační karty. V úvahu připadá pouze obdélníková (eventuelně kruhová) smyčková anténa.

Jakmile používáme v obvodu VF napětí o větší frekvenci jak 1 MHz, již ho nelze považovat za stacionární, ale za elektromagnetickou vlnu. Pokud bychom vedli energii v pásmu HF k cívce antény pomocí dvou nestíněných vodičů, docházelo by k množství nežádoucích vlivů, jako například odrazy energie na VF vedení, impedanční transformace a parazitní vyzařování. V systémech RFID se obecně používá koaxiální vedení i konektory s impedancí 50 Ω . Na Obrázek 3.1: Obecné připojení RFID antény k vysílači [2]. je obecné schéma připojení RFID antény.

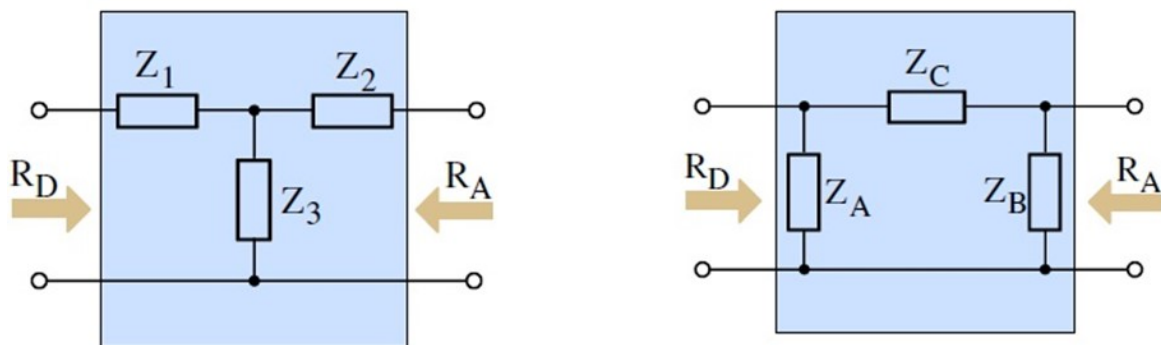


Obrázek 3.1: Obecné připojení RFID antény k vysílači [2].

Víme, že naše anténa X_{LS} je paralelní rezonanční obvod (PRO). Nosný kmitočet 13,56 MHz je neměnný a anténa je naladěna do rezonance. PRO při rezonanci má minimální impedanci, přičemž platí $X_L = X_C$. Pro impedanci PRO platí vztah

$$Z_0 = jX_L - jX_C + R_L = R_L \quad (3.1)$$

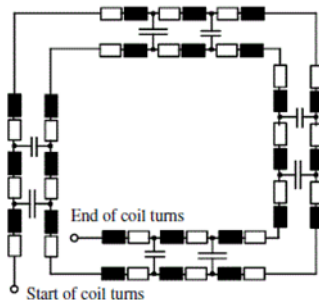
Výsledná impedance je tedy rovna pouze reálnému odporu vinutí indukčnosti čili maximálně několik Ω bez imaginární složky. Proto se musí tato anténa dodatečně opatřit impedančním přizpůsobovacím obvodem (matching circuit) na 50 Ω nebo na takovou hodnotu, aby impedančně navazovala na další obvody směrem k vysílači RFID čtečky. Anténu lze obecně přizpůsobit použitím LC prvků. Zapojení můžeme vidět na Obrázek 3.2.



Obrázek 3.2: Nejčastější topologie impedančního přizpůsobovacího obvodu [3].

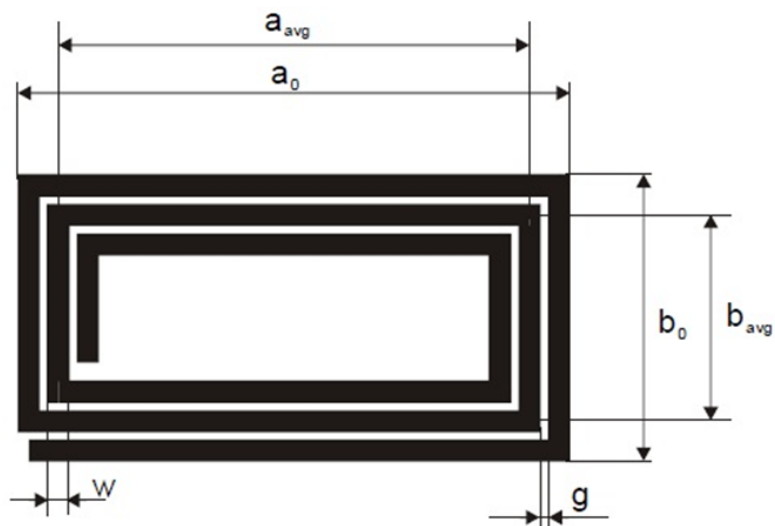
3.1 Výpočet indukčnosti

[4] Jako první je tedy nutné výpočtem určit indukčnost plošné (planární) cívky. Jelikož reálná cívka je vlastně elektrické vedení s rozloženými parametry (Obrázek 3.3), je detailní výpočet poměrně složitý, protože se musí započítávat interakce každého úseku vodiče s těmi ostatními. Jejich magnetická pole se totiž vzájemně protínají.



Obrázek 3.3: Reálné vlastnosti planární cívky.

Postup, který jsem použila, je zjednodušený, ale s uspokojivou přesností. Nesmíme ale zapomínat, že se na tuto anténu musíme dívat komplexně. Jelikož obsahuje množství vzájemných LC vazeb, má také vlastní rezonanční frekvenci (je jich určitě více) v oblasti desítek až stovek MHz.



Obrázek 3.4: Typická planární obdélníková anténa [4].

Proměnné:

a_0, b_0 (Vnější rozměry cívky) – 0,182 m; 0,142 m

t (Tloušťka vedení) – 0,000 035 m

w (Šířka vedení) – 0,002 m

g (Mezera mezi vedením [m]) – 0,003 m

N_a (Počet závitů) – 4z

a_{avg}, b_{avg} (Střední rozměr vinutí) – [m]

d (Ekvivalentní průměr vodiče) – [m]

Výpočet ekvivalentního průměru vodiče vinutí [4]

$$d = \frac{2(t+w)}{\pi} = \frac{2(35 \cdot 10^{-6} + 2 \cdot 10^{-3})}{\pi} = 1,3 \text{ mm} \quad (3.2)$$

Střední rozměr ve směru „a“ [4]

$$a_{avg} = a_0 - N_a \cdot (g + w) = 0,182 - 4 \cdot (0,003 + 0,002) = 0,162 \text{ m} \quad (3.3)$$

Střední rozměr ve směru „b“ [4]

$$b_{avg} = a_0 - N_a \cdot (g + w) = 0,142 - 4 \cdot (0,003 + 0,002) = 0,122 \text{ m} \quad (3.4)$$

Mezivýpočet pro skupinu vodičů 1 [4]

$$x_1 = a_{avg} \cdot \ln \left[\frac{2 \cdot a_{avg} \cdot b_{avg}}{d \cdot (a_{avg} + \sqrt{a_{avg}^2 + b_{avg}^2})} \right] = 0,162 \cdot \ln \left[\frac{2 \cdot 0,162 \cdot 0,122}{0,0013 \cdot (0,162 + \sqrt{0,162^2 + 0,122^2})} \right] = 0,717 \quad (3.5)$$

Skupina vodičů 2 [4]

$$x_2 = b_{avg} \cdot \ln \left[\frac{2 \cdot a_{avg} \cdot b_{avg}}{d \cdot (b_{avg} + \sqrt{a_{avg}^2 + b_{avg}^2})} \right] = 0,122 \cdot \ln \left[\frac{2 \cdot 0,162 \cdot 0,122}{0,0013 \cdot (0,122 + \sqrt{0,162^2 + 0,122^2})} \right]$$

$$x_2 = 0,554 \quad (3.6)$$

Skupina vodičů 3 [4]

$$x_3 = 2 \cdot \left[a_{avg} + b_{avg} - \sqrt{a_{avg}^2 + b_{avg}^2} \right] = 2 \cdot \left[0,162 + 0,122 - \sqrt{0,162^2 + 0,122^2} \right] = 0,162 \quad (3.7)$$

Skupina vodičů 4 [4]

$$x_4 = \frac{a_{avg} + b_{avg}}{4} = \frac{0,162 + 0,122}{4} = 0,071 \quad (3.8)$$

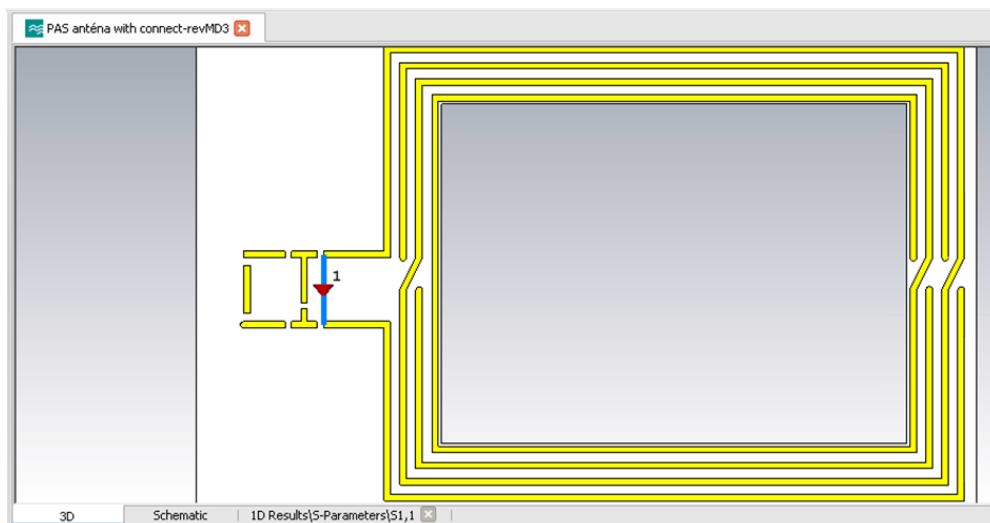
Výsledná indukčnost plošné cívky [4]

$$L_a = \frac{\mu_0}{\pi} \cdot [x_1 + x_2 - x_3 + x_4] \cdot N_a^{1,8} = \frac{4\pi \cdot 10^{-7}}{\pi} \cdot [0,717 + 0,554 - 0,162 + 0,071] \cdot 4^{1,8} = 5,72 \mu H \quad (3.9)$$

3.2 Výpočet indukčnosti v CST Studiu

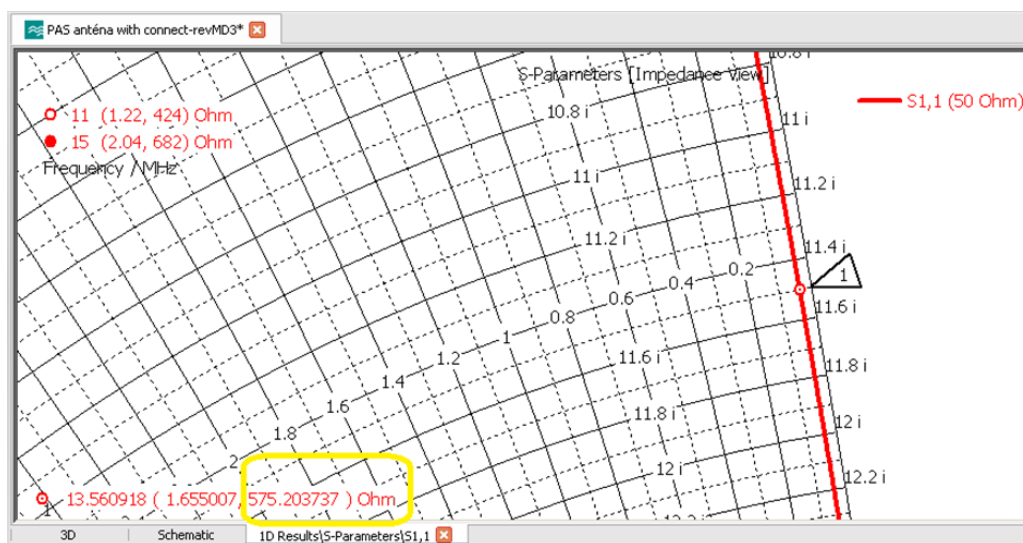
[18][4] Abychom se teoretickým výpočtem co nejvíce přiblížili skutečnosti, je třeba ho zopakovat jinými metodami. Simulační program CST Studio provádí výpočty s mnohem větší diskretností a přesnějšími parametry okolního prostředí. Jen vytvoření projektu je mnohem

složitější. Simulovala jsem pouze samotnou planární indukčnost. Použila jsem cuprexitovou desku tloušťky 1,5 mm z nosného substrátu FR-4 s měděnou vrstvou tloušťky 35 μm .



Obrázek 3.5: 3D model antény.

Výsledkem je Smithův diagram S11 s frekvenčními charakteristikami (Obrázek 3.6). Z grafu se v bodu „1“ dá velice přesně odečíst induktivní reaktance, ze které vypočítám samotnou indukčnost.



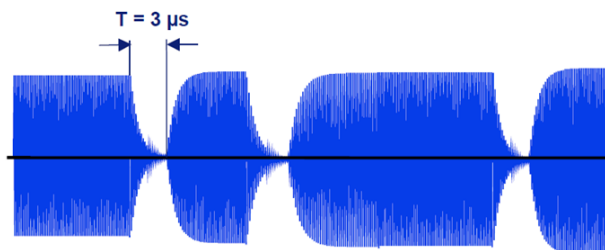
Obrázek 3.6: S11 parametry planární cívky.

Výpočet indukčnosti:

$$L = \frac{X_L}{2\pi f} = \frac{575}{2\pi \cdot 13,56 \cdot 10^6} = 6,75 \mu\text{H} \quad (3.10)$$

Další výpočty jsou prováděny již s tímto výsledkem, protože předpokládám, že je přesnější. Bohužel CST studio sice počítá matematicky přesně, ale reálná hodnota je silně ovlivněna vlastnostmi substrátu. Ty se mohou měnit kus od kusu, protože se nejedná o speciální výrobek, a tak za dodržování shodné permitivity výrobce neručí.

Nyní musíme snížit jakost antény Q_a na takovou hodnotu, kterou potřebujeme pro přenos amplitudově modulovaného signálu. Norma ISO14443-2 [1], která určuje parametry modulovaného signálu pro cestovní doklady, určuje maximální šířku impulsu $T_i \leq 3 \mu s$ při přenosové rychlosti 106 kbps.



Obrázek 3.7: Modulace ASK při přenosu typu A ISO14443.

Pro šířku přenášeného pásma v impulsním provozu platí vztah: $B \cdot T_i \geq 1$

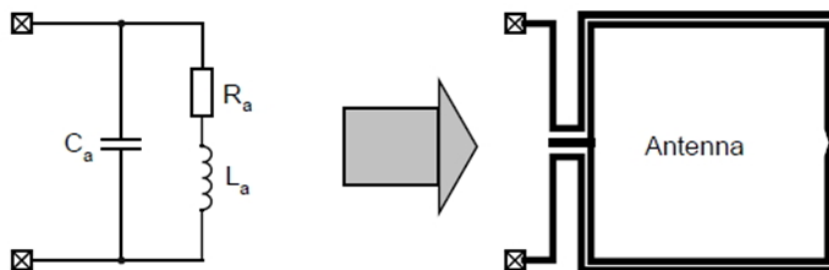
Vztah mezi šířkou pásma a jakostí zase udává vztah: $B = f / Q$

Sloučením obou vztahů dostaneme vzorec pro námi požadovanou jakost: [4]

$$Q \leq f \cdot T_i \leq 13,56 \cdot 10^6 \cdot 3 \cdot 10^{-6} \leq 40$$

Protože ale musíme vzít v úvahu i subnosné frekvence, výrobce doporučuje $Q \leq 35$.

Ten totiž kromě nosné 13,56 MHz může používat ještě subnosnou frekvenci 847 kHz. Snížení jakosti můžeme provést přidáním malého odporu do série s anténou. Protože ale počítáme diferenciální anténu, musíme odpor snižující jakost rozložit na dva stejné odpory R_Q .



Obrázek 3.8: Schéma zapojení pro snížení Q_a [4].

Jakost rezonančního obvodu:

$$Q = \frac{\omega L}{R} \quad (3.11)$$

Výpočet dampingových (tlumících) odporů: [4]

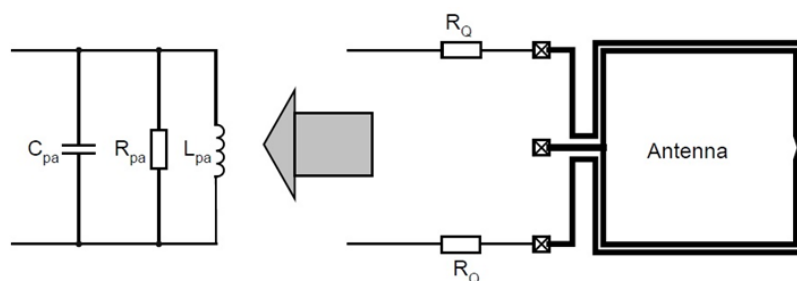
$$R_Q = \frac{\left(\frac{\omega L_a}{35} - R_a\right)}{2} = \frac{\left(\frac{85,2 \cdot 10^6 \cdot 6,75 \cdot 10^{-6}}{35} - 0,82\right)}{2} = 7,5 \, \Omega \cong 7,33 \, \Omega \quad (3.12)$$

$R_A = 0,82 \, \Omega$ – reálný odpor vinutí antény

R_Q – dva přidané odpory pro snížení jakosti (dampingový odpor)

Q – požadovaná jakost cívky ≤ 35

$\omega = 2\pi f_0 = 85,2 \cdot 10^6$ – úhlová frekvence nosného signálu



Obrázek 3.9: Převod na paralelní tlumící odpor [4].

Z důvodu dalších výpočtů musíme přepočítat hodnotu předřadného odporu R_Q na paralelní tlumící odpor R_{Pa} [4]

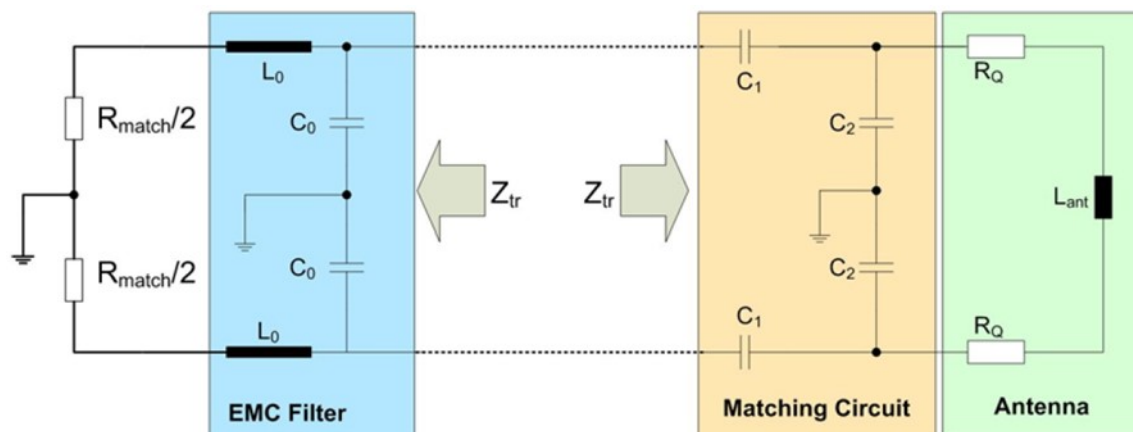
$$R_{Pa} = \frac{(\omega L_a)^2}{R_a + 2R_Q} = \frac{(85,2 \cdot 10^6 \cdot 6,75 \cdot 10^{-6})^2}{0,82 + 2 \cdot 7,33} = 21,4 \, k\Omega \quad (3.13)$$

Základní vztah pro výpočet rezonanční frekvence

$$\omega = \frac{1}{\sqrt{L \cdot C}} \quad (3.14)$$

Výpočet velikosti rezonanční kapacity C_{Pa} pro samostatnou anténu jako PRO [4]

$$C_{Pa} = \frac{1}{\omega^2 \cdot L_a} = \frac{1}{(85,2 \cdot 10^6)^2 \cdot 6,75 \cdot 10^{-6}} = 20,4 \, pF \quad (3.15)$$



Obrázek 3.10: Propojení vysílač – anténa a jejich přizpůsobení [4].

Dále spočítáme EMC filtr, což je vlastně dolnoproustný filtr, který má za úkol propustit pouze frekvence do velikosti nosné 13,56 MHz navýšené o subnosnou 848 kHz, tj. $f_{r0} \cong 14,4 \text{ MHz}$. Jeho význam je v tom, že brání průniku vyšších harmonických frekvencí z výstupů procesoru ven do antény. Výstupy totiž pracují ve spínaném režimu a nemají tedy sinusový, ale pravoúhlý tvar. Pravoúhlý signál obsahuje značné množství harmonických násobků a ty by mohly způsobovat rušení jiných zařízení. Jako L_0 se doporučuje indukčnost v rozmezí 390 nH – 1 μH . Dosadím hodnotu použitou v modulu PN532 V3-1, ke kterému budu anténu připojovat, kde $L_2 = 560 \text{ nH}$.

Výpočet kapacity pro dolnofrekvenční propustnost EMC filtru [4]

$$L_0 = 560 \text{ nH}$$

$$C_0 = \frac{1}{(2\pi f_{r0})^2 \cdot L_0} = \frac{1}{(2\pi 14,4 \cdot 10^6)^2 \cdot 560 \cdot 10^{-9}} = 218 \text{ pF} \cong 220 \text{ pF} \quad (3.16)$$

Výsledná hodnota se po zaokrouhlení shoduje s kapacitou $C_9 = 220 \text{ pF}$, která je na desce modulu PN532 V3-1 (Obrázek 5.1).

K dokonalému přizpůsobení antény a vysílače, aby se co nejefektivněji vysílala do prostoru všechna energie, je nutné vykompenzovat jalové složky impedance. To znamená, jak je vidět na předchozím Obrázek 3.10, že impedance počítaná ze směru od vysílače, musí být komplexně sdružená k impedanci počítané ze směru od antény. Potom se tyto komplexní složky vzájemně vyruší a zůstane jen ta reálná.

Velikost impedance ve směru od procesoru za EMC filtrem [4]

$$Z_{tr} = R_{tr} + jX_{tr} \quad (3.17)$$

Impedance přizpůsobovacího obvodu včetně antény [4]

$$Z_{tr}^* = R_{tr} - jX_{tr} \quad (3.18)$$

$R_{match} = 40 \, \Omega$ – odpor mezi výstupy TX1 a TX2 procesoru PN532 (údaj výrobce Data sheet PN532/C1 str. 196). Nyní tedy vypočítáme reálnou a imaginární část impedance antény ve směru od procesoru RF čtečky za EMC filtrem.

Reálná část impedance za EMC filtrem [4]

$$R_{tr} = \frac{R_{match}}{(1 - \omega^2 \cdot L_0 \cdot C_0)^2 + \left(\omega \cdot \frac{R_{match}}{2} \cdot C_0\right)^2} = \frac{40}{(1 - (85,2 \cdot 10^6)^2 \cdot 560 \cdot 10^{-9} \cdot 220 \cdot 10^{-12})^2 + \left(85,2 \cdot 10^6 \cdot \frac{40}{2} \cdot 220 \cdot 10^{-12}\right)^2} = 264 \, \Omega \quad (3.19)$$

Imaginární část impedance za EMC filtrem [4]

$$X_{tr} = 2\omega \cdot \frac{L_0 \cdot (1 - \omega^2 \cdot L_0 \cdot C_0) - \frac{R_{match}^2}{2} \cdot C_0}{(1 - \omega^2 \cdot L_0 \cdot C_0)^2 + \left(\omega \cdot \frac{R_{match}}{2} \cdot C_0\right)^2} = 2 \cdot 85,2 \cdot 10^6 \cdot \frac{560 \cdot 10^{-9} \cdot (1 - (85,2 \cdot 10^6)^2 \cdot 560 \cdot 10^{-9} \cdot 220 \cdot 10^{-12}) - \frac{40^2}{2} \cdot 220 \cdot 10^{-12}}{(1 - (85,2 \cdot 10^6)^2 \cdot 560 \cdot 10^{-9} \cdot 220 \cdot 10^{-12})^2 + \left(85,2 \cdot 10^6 \cdot \frac{40}{2} \cdot 220 \cdot 10^{-12}\right)^2} = -32,4 \, \Omega \quad (3.20)$$

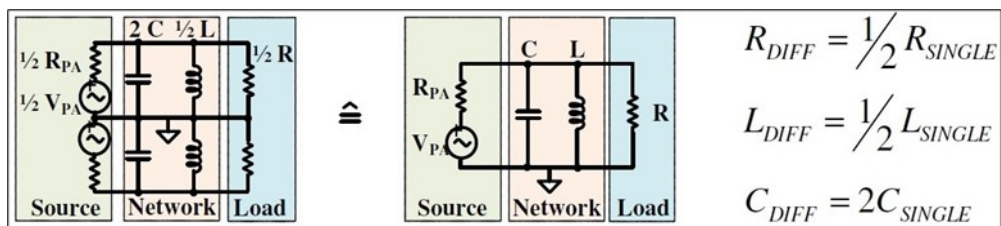
Výpočet sériové kapacity impedancečního přizpůsobení antény C_1, C_2 [4]

$$C_1 = \frac{1}{\omega \cdot \left(\sqrt{\frac{R_{tr} \cdot R_{pa}}{4} + \frac{X_{tr}}{2}}\right)} = \frac{1}{85,2 \cdot 10^6 \cdot \left(\sqrt{\frac{264 \cdot 21400}{4} + \frac{-32,4}{2}}\right)} = 10 \, pF \quad (3.21)$$

Paralelní (rezonanční) kapacita antény se zohledněním vlivu vysílače [4]

$$C_2 = \frac{1}{\omega^2 \cdot \frac{L_{pa}}{2}} - \frac{1}{\omega \cdot \sqrt{\frac{R_{tr} \cdot R_{pa}}{4}}} - 2C_{pa} = \frac{1}{(85,2 \cdot 10^6)^2 \cdot \frac{6,75 \cdot 10^{-6}}{2}} - \frac{1}{85,2 \cdot 10^6 \cdot \sqrt{\frac{264 \cdot 21400}{4}}} - 2 \cdot 20,4 \cdot 10^{-12} = 9,9 \, pF \cong 10 \, pF \quad (3.22)$$

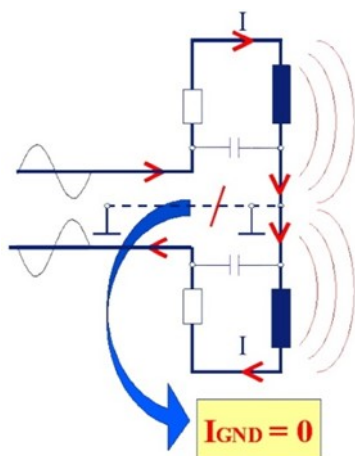
Protože se rezonance antény bude jemně doladovat pomocí kapacitního trimru, bude nejlepší nahradit oba kondenzátory C_2 diferenciální antény pouze jedinou součástkou, podle následujícího schématu (Obrázek 3.11). Budeme tedy potřebovat kapacitní trimr s hodnotou $C_{tr} = 10,3 \, pF / 2 \geq 6 \, pF$. Kapacitu nebudeme uzemňovat, necháme uzemněný pouze střed vinutí antény. Vinutí obou antén musí být sousa a pokud možno v co nejtěsnější magnetické vazbě mezi sebou. [3]



Obrázek 3.11: Transformace hodnot součástek mezi diferenciální a sigle anténou [3].

Pokud budeme mít symetrickou a správně vykompenzovanou anténu, potom proud přes zem bude roven nule (Obrázek 3.12). Propojení stínění se středem vinutí bude mít za úlohu pouze vyrovnání stejnosměrných potenciálů a správné impedanční zakončení koaxiálního vedení.

Jelikož chci anténu napájet dvěma samostatnými koaxiálními kabely stejné délky, nepoteče stíněním žádný proud. Lze použít také tzv. triaxiál, což jsou vlastně dva koaxiály v jednom, ale komplikuje se to zase použitím speciálního konektoru, který se mi nepodařilo sehnat.



Obrázek 3.12: Vykompenzovaná anténa [4].

Mohlo by se sice zdát, že mezi oběma živými napájecí antény bude dvojnásobné napětí (při napájení procesoru 3,3 V tedy 6,6 V) a výkon antény by mohl stoupnout 4x. Ale impedance mezi nimi je dvojnásobná, takže zdvojením antény na diferenciální stoupne výstupní výkon pouze 2x.

Vzorec navýšení výkonu signálu

$$P_{tot} = \frac{(2U)^2}{2Z_0} = 2 \left(\frac{U^2}{Z_0} \right) = 2P_0 \quad (3.23)$$

3.3 Simulace v programu Smith v4.1

[7][4] Dále jsem pro zpřesnění výpočtů impedančního přizpůsobení použila program Smith v4.1, který se mi pro samotný návrh celého zapojení osvědčil jako daleko pružnější a přívětivější. Musí se započítat všechny prvky, včetně EMC filtru, který značně ovlivňuje výsledné hodnoty. Problém je, že EMC filtr zůstává součástí modulu RFID čtečky, který budu používat pro praktické ověření funkčnosti antény a nejsem schopna tyto součástky doladit, protože jsou v rozměrech SMD0603 (tj. 1,55 x 0,85 mm). Beru je tedy jako konstantní.

Schéma zapojení zadaného do programu Smith vychází z Obrázek 3.10, jen jsou hodnoty upravené podle přepočtu na Obrázek 3.11 na single anténu. Jako anténu jsem zadala prvek s impedancí vypočítanou podle vztahu:

$$X_L = R_q + j \frac{X_L}{2} = 7,3 + j \frac{575}{2} = (7,3 + j287,5) \Omega$$

Další součástky jsou vloženy v tomto pořadí i když jejich hodnoty jsou již výsledkem ladění:

- Paralelní (rezonanční) kapacita 29,3 pF
- Sériová kapacita impedančního přizpůsobení 12 pF
- Paralelní kapacita EMC filtru 220 pF (konstantní)
- Sériová indukčnost EMC filtru 560 nH (konstantní)

Pracovní frekvence se nastaví na 13.56 MHz. V políčku „Default Z_0 “ nastavím hledaných 20 Ω (vysvětlím následovně), protože k této hodnotě se vztahují například kružnice činitele odrazu SWR.

V položce „Sweep“ nastavíme následující hodnoty:

- Startovní frekvence 11.56 MHz
- Konečná frekvence 15.56 MHz
- Krok 100 kHz

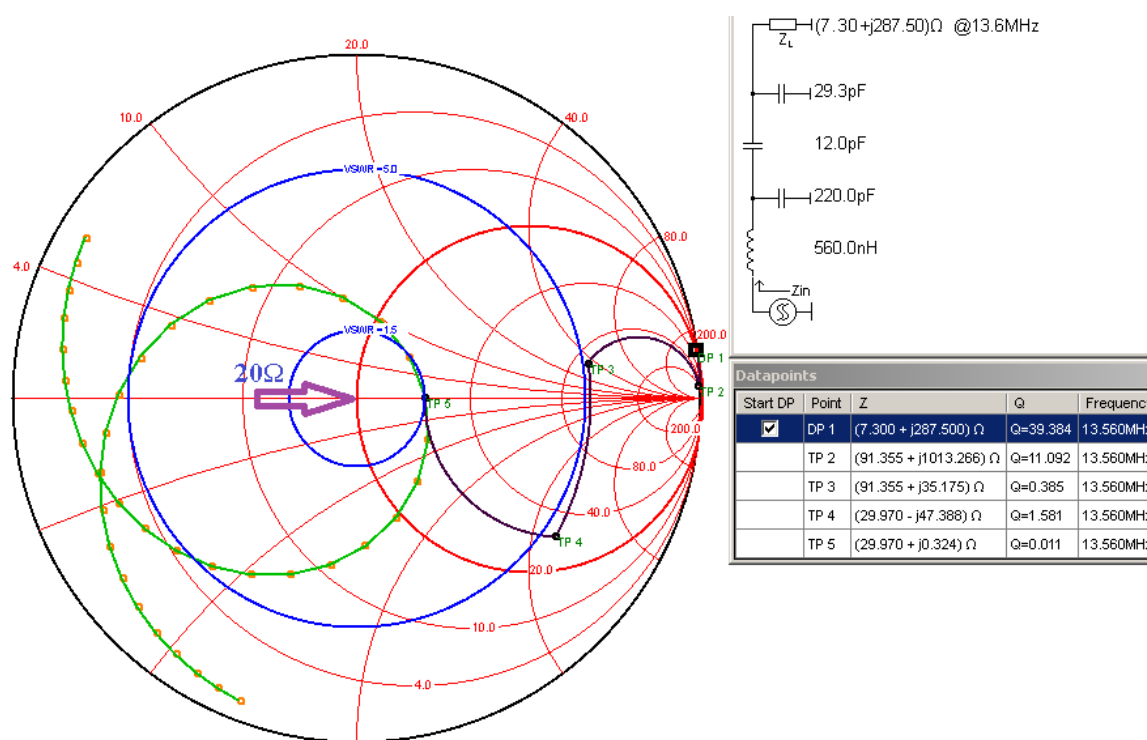
Tlačítko „Drive“ nám do grafu vykreslí křivku frekvenční závislosti vstupní impedance – tedy na straně připojení TX výstupu RFID vysílače PN532. Na Obrázek 3.13 je vidět výsledek simulace. Zelená křivka v diagramu je frekvence, uprostřed s hodnotou 13,56 MHz – s krokem 100 kHz. Můžeme si všimnout, že obě subnosné frekvence ± 847 kHz spadají až do SWR = 5.

V technické specifikaci [5] je uvedený odpor mezi jednotlivými výstupy TX1 a TX2 40 Ω . Když ale budeme uvažovat pouze jeden, jako single výstup, bude mít proti zemi maximálně 20 Ω . Výrobce NXP Semiconductors doporučuje při jemném ladění pomocí Smithova diagramu nastavit odpor 23 Ω , což zahrnuje nepřesnosti v nastavení parametrů antény

případně zatížení antény RFID tagem. Tlačítkem „Tune“ lze doladit impedanci celé antény jednotlivými součástkami. V mém případě jsem doladila dvě kapacity u antény. Cílem tedy je dostat výslednou impedanci na hodnotu $R = 23 \, \Omega$ reálných. Nápomocné může být to, že rezonanční kapacita (první shora) pohybuje frekvenčně závislou smyčkou nahoru a dolů, mezi induktivní a kapacitní reaktancí a přizpůsobovací kondenzátor (uprostřed) ovlivňuje velikost této smyčky. Ideálně by smyčka měla být symetrická podle reálné osy, ale to se dá doladit pouze součástkami v EMC filtru.

Poměrně malým rozladěním antény dochází k drastickému poklesu reálného odporu. V místě křížení zelené frekvenční charakteristiky je $R = 2,5 \, \Omega$ a oběma směry dále klesá odpor až pod $1 \, \Omega$. Doladíme impedanci pro vysílání nosného signálu, ale když si odečteme \pm frekvenci subnosné 847 kHz, uvidíme, že pro tyto kmitočty má anténa impedanci pouze $4 \, \Omega$. Myslím si, že doladění antény v reálných podmínkách, nejlépe za přítomnosti subnosné frekvence, je přímo nutné. Musíme ji nastavit na maximální dosah komunikace. Při práci srozladěnou anténou je možné tímto způsobem mikroprocesor i zničit.

Zároveň se s tím váže také jeden problém mého návrhu. Jelikož jsem nesehnala RFID čtečku s výstupní impedancí $50 \, \Omega$, musela jsem se přizpůsobit modulu PN532. Kdybych naopak chtěla obě součásti (anténu i EMC filtr) doladit na $50 \, \Omega$, bylo by to na úkor značného útlumu celé trasy.



Obrázek 3.13: Dolad'ování prvků pomocí Smithova diagramu (nepřesné doladění).

Podle výsledků simulace je v místě spojení EMC filtru a anténní části impedance cca 110 Ω . Ale protože od samého počátku uvažuji o anténě jako o samostatném modulu, který by se připojoval pomocí dvou koaxiálních kabelů 50 Ω , musela jsem původně dlouhé kabely zkrátit, aby vedení co nejméně ovlivňovalo výslednou impedanci. Vlnová délka $\lambda/2$ je 11 m. Délka kabelu se dá také doladit ve Smithově diagramu. Protože je anténa diferenciální a přesně symetrická, budou VF proudy protékat pouze živými vodiči koaxiálních kabelů, stíněním ne.

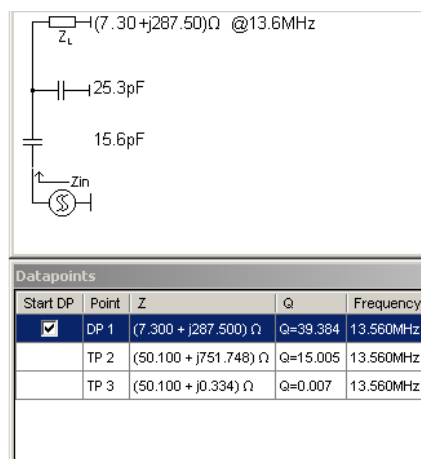
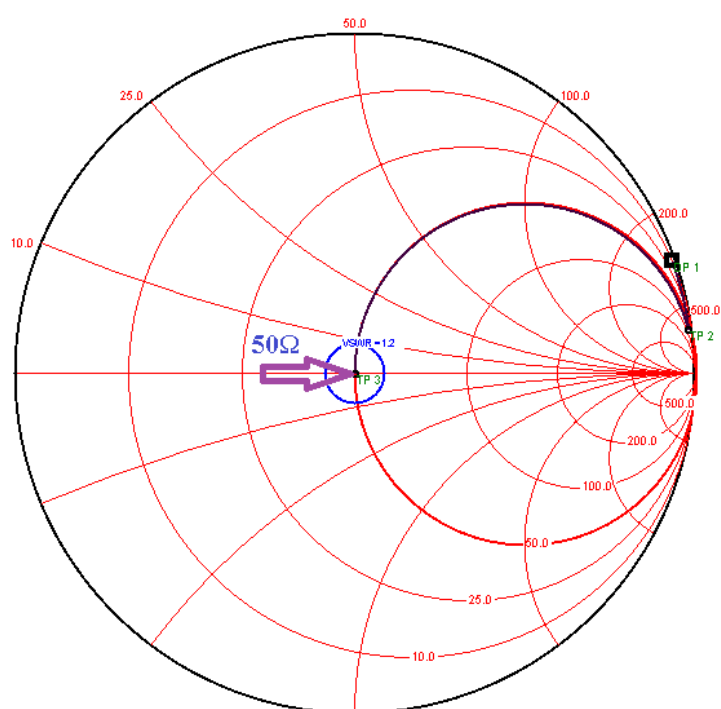
Do zapojení ve Smithově diagramu jsem tedy započítala i koaxiální kabel. Je ale třeba nejprve nastavit parametry tohoto vedení. Přesné parametry kabelu RG58C/U jsem odvodila z tabulky výrobce[8]:

- Charakteristická impedance $Z_0 = 50 \Omega$
- ϵ_r – činitel zkrácení – poměr rychlosti světla k rychlosti šíření signálu koaxiálním kabelem. Tabulka uvádí 65,9 % rychlosti světla, tj. $1/0,659 = 1,517$
- Koeficient α – útlum kabelu v dB/m. Podle tabulky je útlum při frekvenci 10 MHz 4,59 dB/100 m, tj. 0,0459dB/m.

Symetrie frekvenčně závislé smyčky, kterou bych nedokázala doladit bez změny v EMC filtru, se mi posunula přesně v požadovaném směru. Takže propojovací koaxiální kabely délky 198 mm se nyní stanou pevnou součástí impedančního přizpůsobení. Bude to ovšem spojení nezaměnitelné a správně fungující pouze mezi těmito dvěma konkrétními komponenty. Toto propojení se dá nazvat jako tzv. „živé“, protože ovlivňuje ostatní parametry – viz Obrázek 4.1.

Pokud s dostatečnou přesností známe všechny parametry antény, potom její úprava na 50 Ω zahrnuje pouze výměnu obou přizpůsobovacích kondenzátorů C_1 **Error! Reference source not found.** Obrázek 3.10) za hodnoty 15,6 pF, jak vyplývá ze Smithova diagramu (

Obrázek 3.14). A potom se musí kapacitním trimrem doladit maximální komunikační dosah. Trimr má pouze 15 pF maximum a z důvodu dostatečné šířky přeladění se k němu musí paralelně přidat další kapacita cca 4,7 pF (výsledná by měla být $25,3 / 2 = 13$ pF). Potom by již neměl být problém prodloužit i koaxiální přívody, protože jak vysílač, tak i anténa budou mít 50 Ω reálných.



Obrázek 3.14: Změna přizpůsobení na 50Ω .

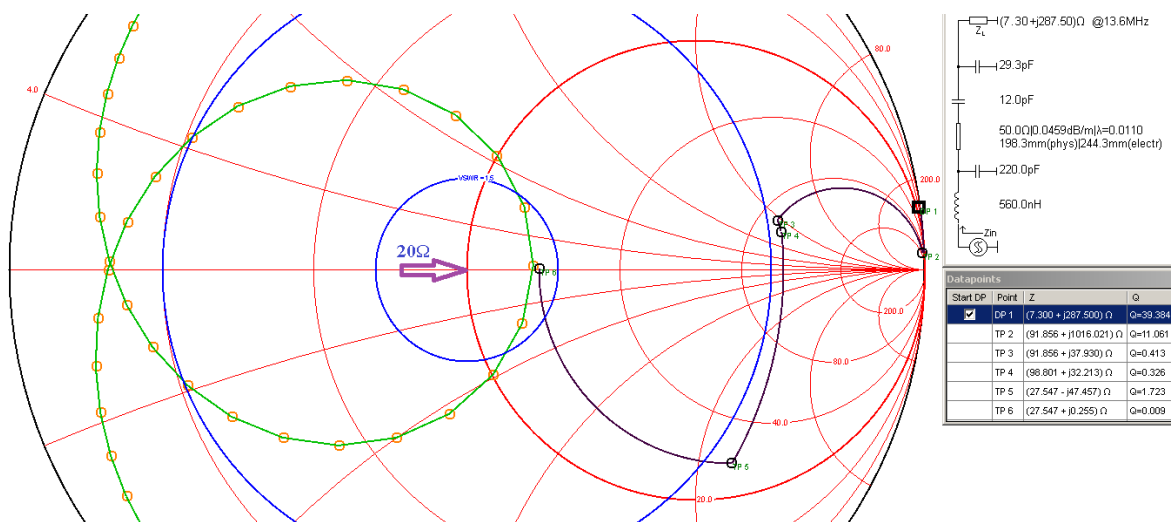
4 Souhrn výsledků simulace

Co se týká návrhu hodnot jednotlivých součástek, považuji za nejpřesnější program Smith v4.1. Nepřesnosti můžou plynout z odchylek v zadaných vstupních hodnotách (v mém případě indukčnosti planární cívky antény) a potom nepřesnosti vlivem tolerance součástek, které se kumulují a za jistých okolností mohou nabýt větších rozměrů. Proto se mi jako nejlepší řešení líbilo použití kapacitního trimru. Současný trend však upřednostňuje volbu jednoduché replikovatelnosti a osazování obvodů pevně stanovenými hodnotami součástek. To je další aspekt, který když započítáme do celkové kvality výrobku, tak nemůže být taková, jak by si autor představoval.

Například když jsem poprvé testovala ještě kompletní modul PN532 V3-1, o kterém píšu níže, a to včetně jeho integrované RFID antény, četl mou testovací MIFARE kartu pouze na vzdálenost 35 mm. Má anténa ji přečte na 100 mm. To je jednoznačný důkaz o špatném naladění, obzvlášť když je v jádru planární antény umístěn celý elektronický obvod. Samotný čip PN532 je určen pro konstrukci čteček do vzdálenosti 50 mm.

Jako finální hodnoty mého návrhu tedy považuji výstup z programu Smith. Indukčnost samotné planární cívky byla nejprve vypočítána ručně jako $5,72 \mu\text{H}$ a potom dodatečně zpřesněna programem CST studio v.2019. Ani tak ale nelze tuto hodnotu brát jako jednoznačnou a trvale platnou vzhledem k rozptylu relativní permitivity substrátu ϵ_r . Pro další výpočty a simulace jsem použila hodnotu z CST studia $L_a = 6,75 \mu\text{H}$ (do programu Smith se zadává pouze jako poloviční hodnota, protože ji musíme přepočítat z diferenciální na single anténu). Dva kondenzátory impedančního přizpůsobení při nejpřesnějším nastavení vychází $11,7 \text{ pF}$. Zaokrouhlila jsem ji na nejbližší sériově vyráběnou hodnotu $C_1 = 12 \text{ pF}$ a zpět dosadila do výpočtu. Jako poslední pak byla znovu zpřesněna rezonanční kapacita programem Smith jako $C_2 = 29,3 \text{ pF}$. Výsledek musíme zase přepočítat zpět na diferenciální anténu. Ta je tvořena vlastně dvěma stejnými, sériově spojenými kapacitami. Výsledek tedy je přibližně 15 pF . Kapacitní trimr, kterým nastavuji tuto hodnotu, má rozsah pouze 15 pF , a proto jsem ho pro jistotu doplnila o dalších $4,7 \text{ pF}$ připojených paralelně.

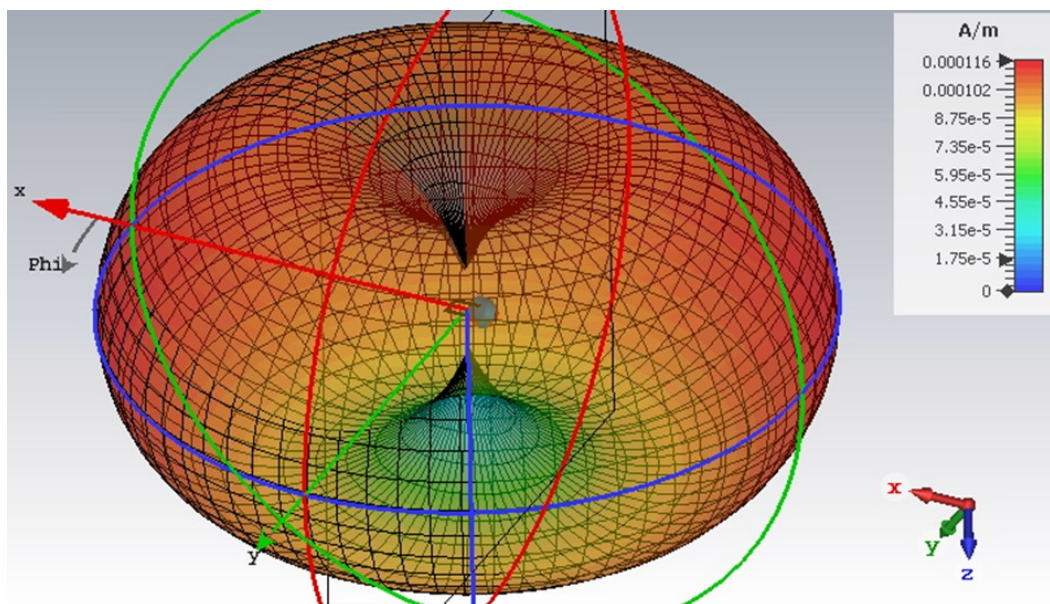
Výsledek není ideální a sice vlivem zaokrouhlení hodnoty C_1 , která má zásadní vliv na velikost činného odporu. Důsledkem této malé změny je, že výsledná impedance není požadovaných 23Ω , ale 27Ω . Je to však zanedbatelná odchylka. Jak je vidět na následujícím Smithově diagramu (Obrázek 4.1), činitel SWR se nijak výrazně nezměnil a je menší jako 1,5 (viz menší modrá kružnice).



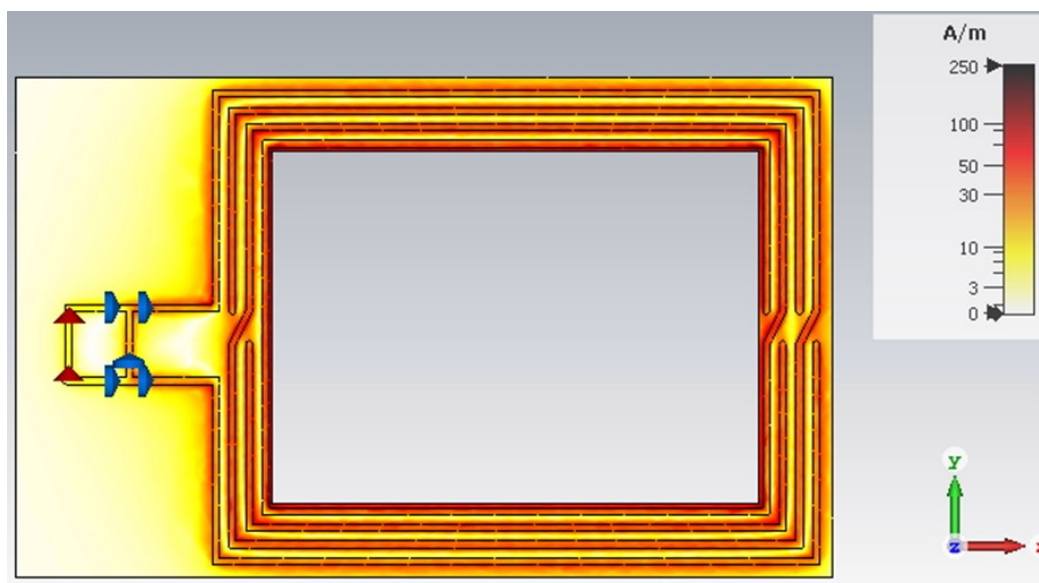
Obrázek 4.1: Správně doladěná anténa k modulu vysílače.

Pro případ, že budeme chtít anténu připojit k vysílači, který má impedančně přizpůsobený výstup na 50Ω , stačí obě kapacity impedančního přizpůsobení vyměnit za hodnotu $C_1 = 15,6 \text{ pF}$ a doladit rezonančním trimrem dosah čtečky na maximální vzdálenost. Anténa se tak stane 50Ω .

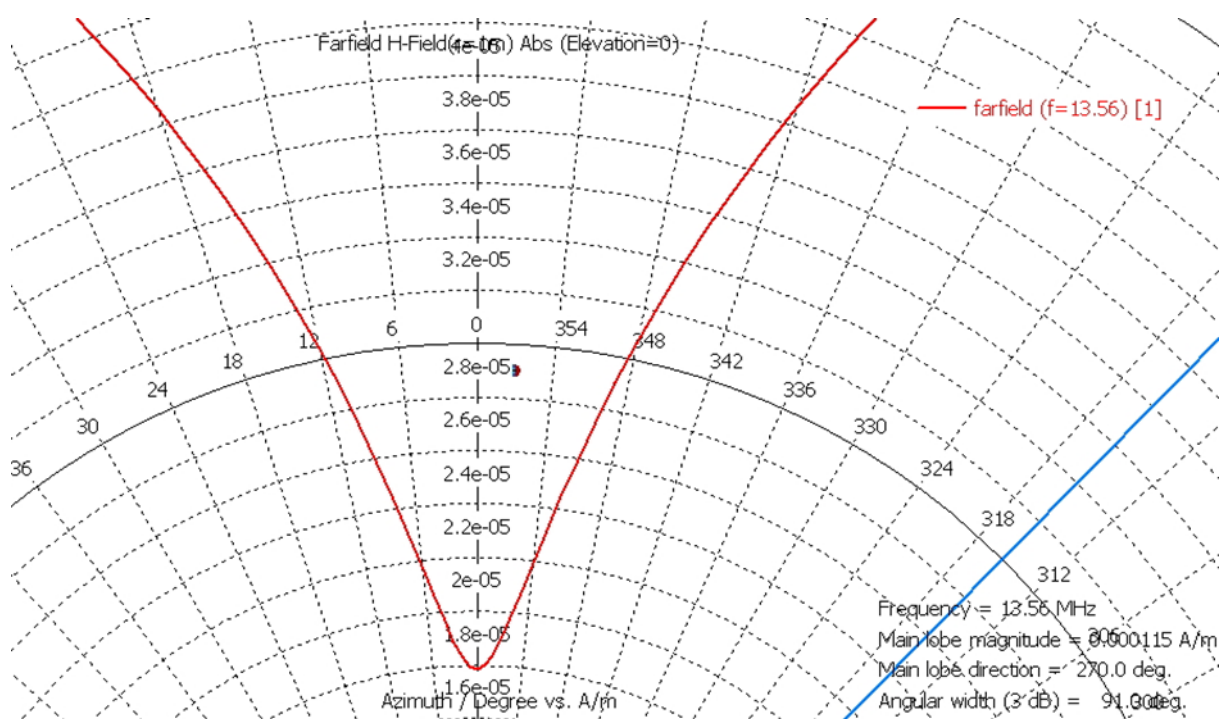
Dalšími výsledky simulace programem CST studio jsou anténní vyzařovací charakteristiky. V rovině desky substrátu má charakteristika stejný tvar tzv. „pneumatiky“, jako klasický dipól kolmý k desce.



Obrázek 4.2: Magnetická vyzařovací charakteristika vzdáleného pole.



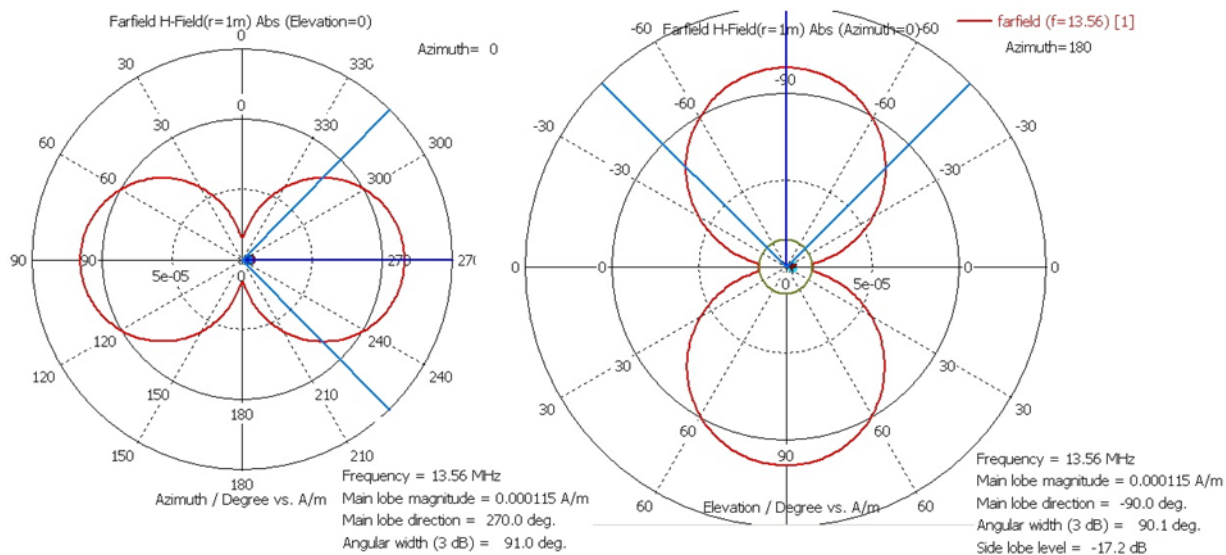
Obrázek 4.3: Rozložení a intenzita magnetického pole na samotném substrátu.



Obrázek 4.4: Propad MP ve středu antény – detail.

Na Obrázek 4.4 je vidět detail „hluchého“ místa nad středem antény, způsobený velkou mezerou mezi vinutím jedné a té protisměrné strany. K útlumu dochází tím, že všechny magnetické siločáry vstupují vrchem směrem do centra cívky. V určité výšce nad cívkou jdou přímo proti sobě. Jednotlivé vektory MP se v tomto prostoru vzájemně odčítají a výrazně tak

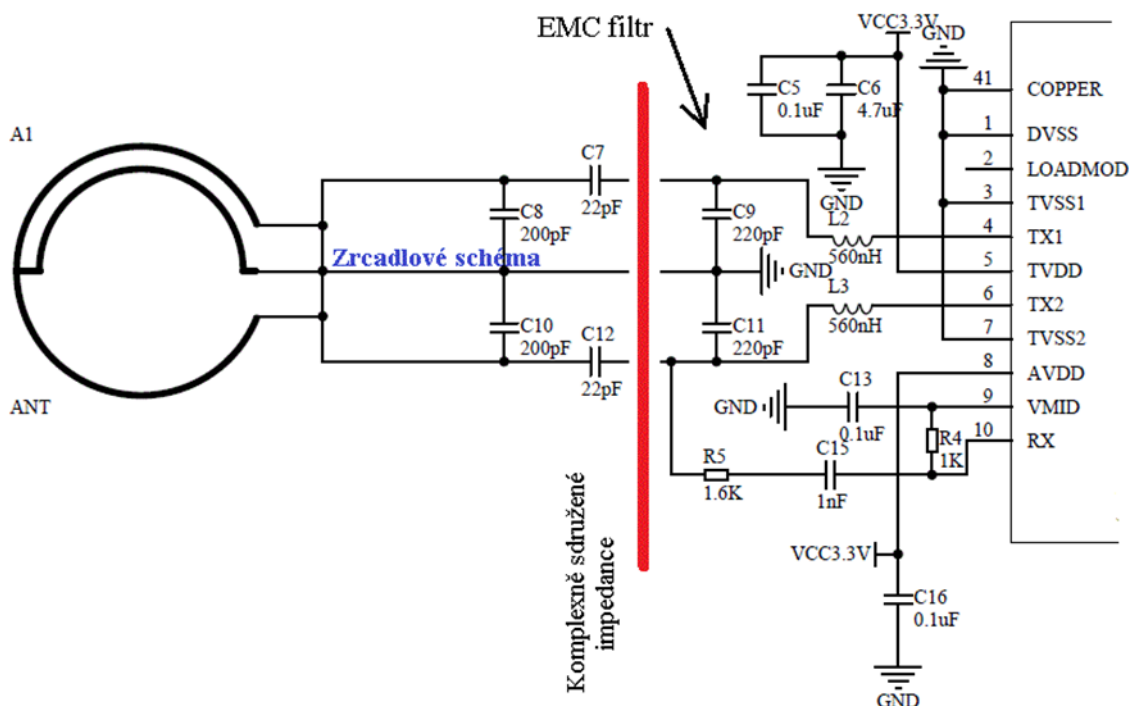
oslabují pole nad středem (na vnějších stranách se naopak sčítají). Na Obrázek 4.5 je vidět, že kdyby se daly od sebe oddělit obě protisměrné strany, pole kolem vinutí by bylo kruhové. Takto se ale vzájemně vystředují a zesilují ve směru roviny substrátu a v opačném směru vzniká propad.



Obrázek 4.5: Vyzařovací charakteristika v obou bokorysech je shodná.

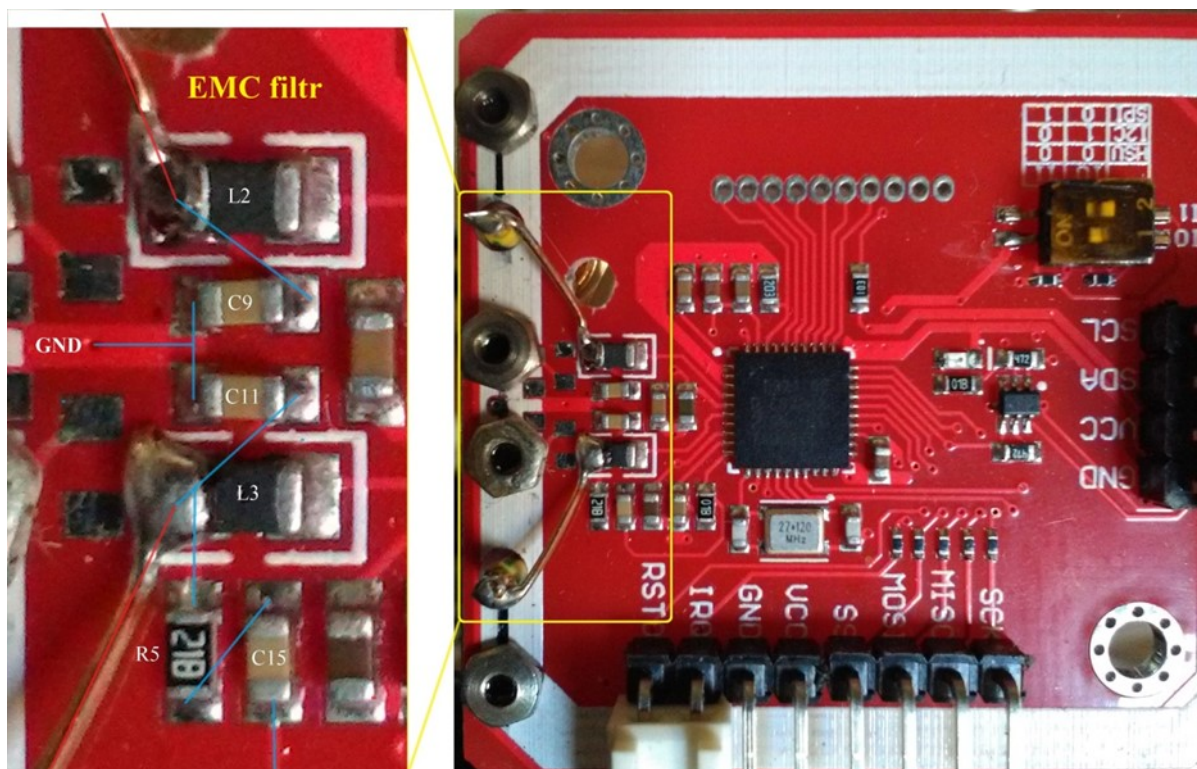
5 Testovací zdroj RFID signálu

[5][25] Kolem návrhu nové RFID antény lze dlouze polemizovat. Myslím si, že nejlepší způsob, jak ověřit funkce antény, je reálné čtení RFID tagů pomocí čtečky, případně porovnání výsledků s jinými anténami. Rozhodla jsem se k tomu použít RFID modul PN532 V3-1, který lze připojit k vývojové desce ARDUINO s procesorem ATMEL MEGA 2560. Drobnou úpravou ukázkového programu z knihovny Adafruit_PN532-1.0.3 jsem vyrobila testovací přístroj, který trvale vytváří nosnou vlnu kolem antény a stále dokola provádí čtení PICC karet MIFARE typu A. Jakmile správně přečte ID, tak se rozsvítí indikační LED a ozve se akustický tón v mini-reproduktoru (cca 1/2sec).



Obrázek 5.1: Dvojčinné zapojení anténní části modulu PN532 V3-1.

Čip PN532 osazený v modulu V3-1, který vyrábí firma NXP Semiconductors, je v současnosti hojně komerčně používán. Podle údajů výrobce lze pomocí tohoto procesoru zkonstruovat čtečku pasivních tagů až do vzdálenosti 50 mm. Protože je však na tomto modulu napevno zapojená a vyleptaná i RFID anténa, bylo třeba na modulu provést drobné změny. Podle následujícího schématu (Obrázek 5.1) byla odpojena anténa a vývody z mikroprocesoru za EMC filtrem byly připojeny na dva pozlacené, koaxiální konektory SMA 50 Ω , ke kterým mohou pomocí koaxiálních kabelů připojit libovolnou RFID anténu.



Obrázek 5.2: HW úprava modulu PN532 V3_1.

Na Obrázek 5.1 je červeně vyznačeno místo oddělení původní antény. Zbytek směrem vlevo je samotná RFID anténa včetně impedančního přizpůsobení. Jak je vidět, anténa se skládá ze dvou, symetrických částí. Je to jednoduchý způsob pro zvýšení výkonu vysílané EM vlny. Výstupy z mikroprocesoru PN532 jsou dva TX1 a TX2, a pracují vzájemně v protifázi. Když je jeden sepnutý, druhý je rozepnutý. Antény, včetně impedančního přizpůsobení, jsou vlastně dvě. Je to tzv. diferenciální nebo také „dvojčinná“ anténa. K samotnému součtu výkonů dochází až na úrovni magnetických polí obou cívek. Takže při napájení mikroprocesoru napětím 3,3 V je magnetické pole celé antény dvojnásobné. Přijímaný signál je z antény odebírán pouze z té dolní větve přes ochranný odpor R5, C15 a pokračuje do vstupu RX. Pokud připojíme pouze dolní polovinu antény a výstup TX1 zůstane nezapojený, čtečka funguje také, jen její dosah se sníží cca o 30 %.



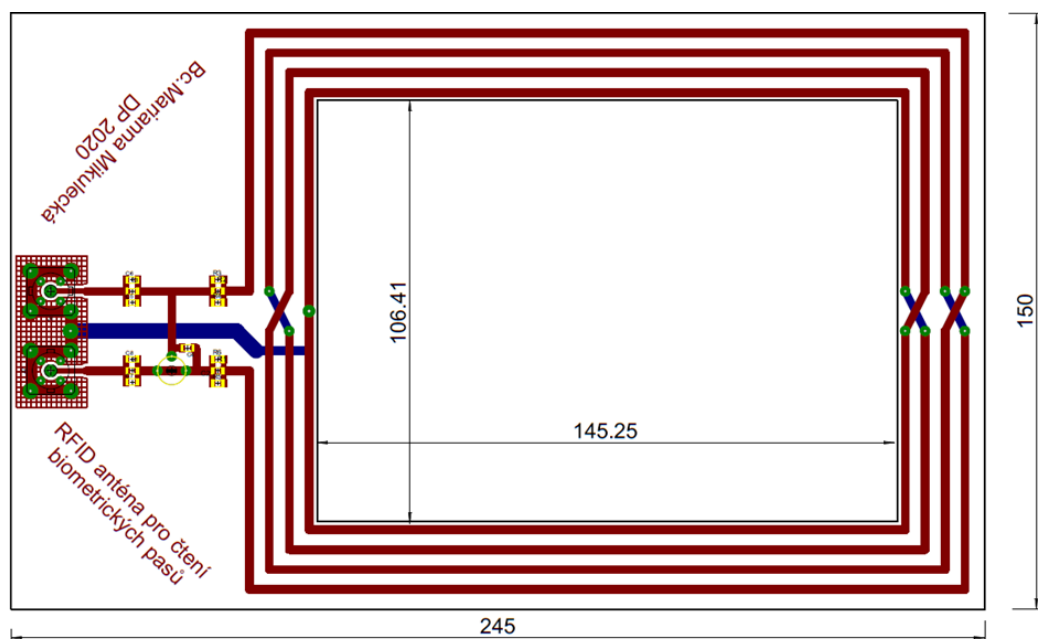
Obrázek 5.3: Pozlacené SMA konektory $50\ \Omega$ použité k propojení antény.



Obrázek 5.4: Propojení Arduino_RFID modul_RFID anténa.

6 Praktická realizace antény

Pro realizaci antény jsem zvolila dostupnou metodu – vytvoření fotografické předlohy na pauzovací papír v programu Eagle, její přenesení pomocí UV lampy na fotocitlivou desku FR-4 tloušťky 1,5 mm, tloušťka Cu vrstvy 35 μm . Po osvitu je nutné fotocitlivou emulzi vyvolat roztokem NaOH (hydroxid sodný), opravit retušovacím lakem a odleptat měděnou vrstvu směsí $\text{H}_2\text{O} + \text{HCl} + \text{H}_2\text{O}_2$ (voda, kyselina chlorovodíková, peroxid vodíku). Po vyleptání a smytí fotocitlivé vrstvy pomocí syntetického ředidla jsem plošný spoj natřela pájecím lakem (roztok kalafuny a lihu). Poté jsem pomocí mikropájky s termostatem a dalšími potřebnými nástroji připájela SMD součástky podle vypočítaných údajů. Kapacitní trimr jsem nejprve provizorně nahradila ladícím kondenzátorem z rádia. Po upřesnění kapacity jsem ho zaměnila za trimr VISHAY s rozsahem do 15 pF, který jsem ale později ještě doplnila o 4,7 pF.

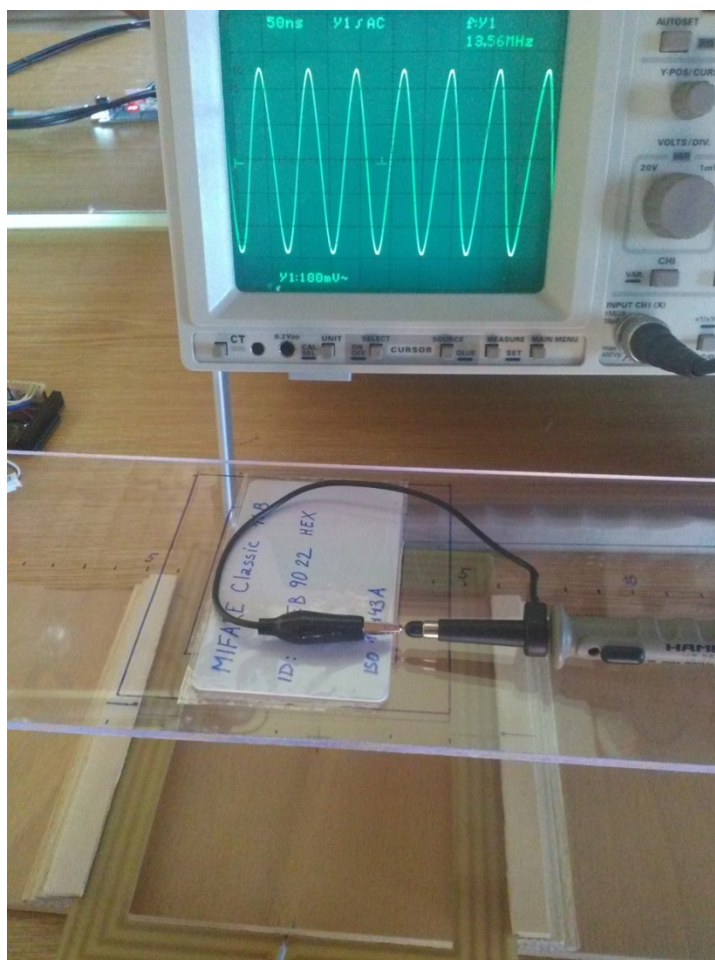


Obrázek 6.1: Schéma RFID antény pro čtení biometrických pasů.

Po připojení antény k RFID modulu jsem za pomoci analogového osciloskopu HAMEG HM504 (100 MHz) naladila maximální amplitudu signálu při rezonanci antény, a sice nepřímou metodou – uzemňovací vodič od sondy osciloskopu jsem spojila s živým, čímž mi vznikla asi 10 cm dlouhá drátová smyčka. Tu jsem pouze přiblížila k RFID anténě, tedy bez elektrického kontaktu, protože jinak by došlo ke značnému ovlivnění parametrů antény vstupními obvody osciloskopu. Na osciloskopu lze zobrazit čistý, harmonický signál 13,56 MHz, který kapacitním trimrem doladíme na maximální amplitudu.

V závěrečné fázi je třeba doladit anténu podle skutečného dosahu. Tuto proceduru nelze nahradit ani výpočtem, ani simulací. Proto jsem potřebovala reálný zdroj signálu RFID čtečky s možností indikace fungující komunikace. NFC kartu MIFARE Classic jsem umístila na

amatérsky vyrobenou lávku z plexiskla, které se považuje za neutrální k elektromagnetické vlně. Nastavení kapacitního trimru z předchozího měření je třeba mít poznačené a finální doladování se musí provádět již v opravdu úzkém rozsahu kolem této hodnoty. Musíme mít k dispozici také dielektrický šroubovák, protože ladící šroub je elektricky spojený s jedním z vývodů kapacitního trimru. Podle údajů výrobce NXP Semiconductors je čip PN532 určen k výrobě NFC čteček do vzdálenosti 50 mm v pasivním režimu. S mojí anténou a kartou se mi podařilo nastavit komunikaci až na vzdálenost 95 mm. Když jsem položila svou „měřicí VF sondu“ až na plošinu s bezkontaktní kartou, je zde patrný i vliv karty samotné na rozložení EM pole. Také jsem objevila skutečnost, že nejspolehlivější komunikace není úplně při maximální amplitudě signálu, ale až při jeho mírném poklesu, a to na obě strany.



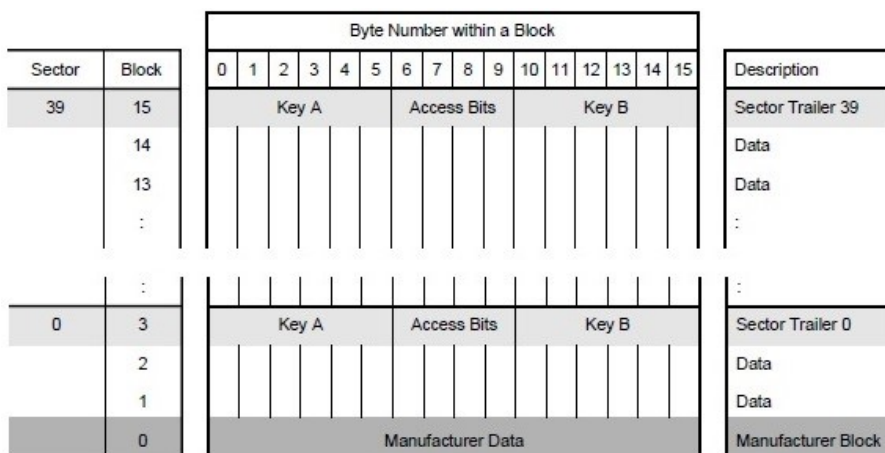
Obrázek 6.2: Ladění antény na "dosah" a improvizovaný detektor EM pole.

Dalším projevem této konkrétní konstrukce antény je její příliš velká plocha. Kvůli nutnosti existence vnitřního otvoru (105 x 145 mm) pro optické skenování strojově čitelné zóny biometrických dokladů nejde vinutí rozložit do spirály. Magnetické siločáry se tedy koncentrují pouze v blízkosti vodičů a ve středu nastává propad. Pro kartu MIFARE s rozměry 50 x 85 mm

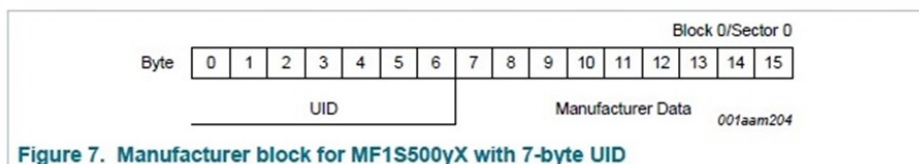
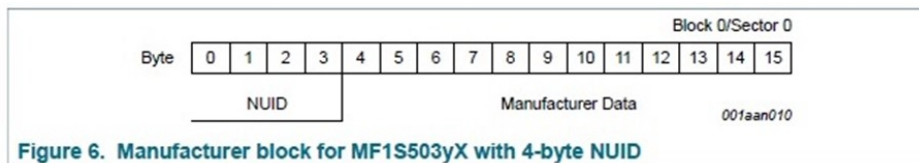
to ale není problém, protože má vinutí též po obvodu a tím se vlastně vyhne největšímu propadu uprostřed. Plastová karta v cestovním pasu má dokonce rozměry 85 x 125 mm. Problém je s menšími výrobky jako klíčenka, protože se musí více přiblížit k obvodu vinutí. Pro toto použití ale anténa není určena.

Poslední záležitost, která mě mrzí, že na mém testeru nefunguje, je čtení samotného biometrického pasu. Prostudovala a vyzkoušela jsem všechny možnosti, které zvládá čip PN532, ale žádný cestovní doklad mi neodpovídá. Na internetu se mi nepodařilo moc podrobností dohledat, protože komunikace s tímto dokladem podléhá jistému utajení. Ani při měření VF pole jsem nezaznamenala jakoukoliv snahu o komunikaci čipu cestovního dokladu ani občanského průkazu. Myslím si, že ke komunikaci je třeba ho teprve nějakým způsobem přimět, stručněji řečeno oslovit ho nějakým specifickým kódem. V několika dokumentech, které jsem při práci studovala, bylo uvedeno, že každá RFID karta se ohlásí svým ID a dalšími technickými údaji od výrobce, nutnými ke komunikaci. Je to adresa 0x00, která je z výroby na pevně nastavena jako „Read Only“. Asi to ale neplatí vždy a také není jisté, že i tento řádek není zašifrovaný, což samo o sobě vylučuje jistotu odpovědi při ozáření nosným signálem. Je jisté, že doklad s optickou strojově čitelnou zónou nebude komunikovat, dokud tuto zónu nepřečteme a nenastavíme šifrovaný přenos tak, jak to PICC čip požaduje. Ale co samotné ID?

[24][9] Pro upřesnění, paměť MIFARE (Obrázek 6.3) je, alespoň na začátku, rozdělena na sektory po čtyřech blocích. Jeden blok = 16 Bytové slovo. Součástí nultého sektoru je také již zmíněná adresa 0x00 s pevně daným obsahem. Adresa 0x04 (poslední blok nultého sektoru) vždy obsahuje dva šesti Bytové klíče A (veřejný), B (tajný) a několik konfiguračních bitů, které jsou z důvodu omezení chybovosti rozděleny do více Bytů. Klíč A v každém sektoru je individuálním přístupovým heslem k celému sektoru. Například v dokumentu [6] je uveden správný algoritmus čtení adresy 0x00 karty MIFARE ve výchozím stavu paměti z výroby: “Proveďte ověření (Authentication) sektoru 0 pomocí výchozího klíče A. Pokud ověření selže, nejedná se o kartu MIFARE”. Oba klíče A i B jsou v “transportním stavu” (z výroby) nastaveny na hodnotu 0xFFFFFFFFFFFF. Podle mé úvahy, když veřejný klíč A nultého sektoru (adr.0x04) změníme, tak bez jeho znalosti nic nepřečteme.



Obrázek 6.3: Paměťová struktura karet MIFARE.



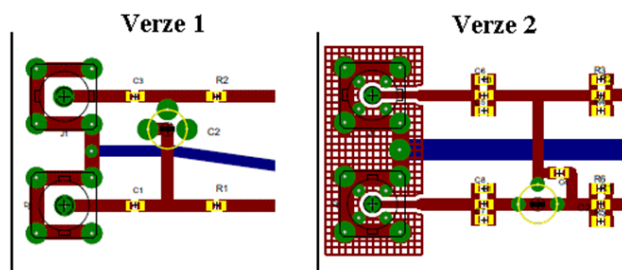
Obrázek 6.4: Začlenění ID.

Předpokládejme, že po úspěšném zalogování cestovního dokladu (nebo po provedení antikolizní procedury) může čtečka zjišťovat jiné údaje, jako např. ID. Čtečka za tímto účelem odešle blok dat s ověřovacími informacemi (mimo jiné i veřejný klíč) pro nultý sektor s požadavkem na přečtení nultého bloku. RFID tag tuto informaci přijme a porovná klíče. Myslím si, že když nedojde ke správnému ověření, nedostane se nám od tagu ani odpovědi ohledně jeho identifikace, že odeslat ID není povinnost. ID je součástí paměti tagu podléhající nastaveným pravidlům.

Protože i firma NXP Semiconductors musí dodržovat nějakou bezpečnostní politiku, je pravděpodobné, že čip PN532 má v sobě implementovaná jistá SW omezení, protože se jedná o komerční výrobek a nedocházelo tak k jeho zneužití.

6.1 Verifikace výsledků

Se vzniklou situací kolem covid-19 jsem měla omezené možnosti měření. Zabezpečit měření se mi podařilo celkem dvakrát, z toho první, v univerzitní laboratoři a druhé na specializovaném pracovišti pro výrobu radiolokační techniky. Vyrobila jsem dvě, téměř identické kopie antény, protože po prvním měření jsem anténu nechala k dispozici svému vedoucímu práce. Odchyly, které mezi těmito verzemi byly, jsou patrné na následujícím obrázku. Typuji, že největší rozdíl je v lepším propojení a zvětšení zemní plošky v místě připojení SMA konektorů.



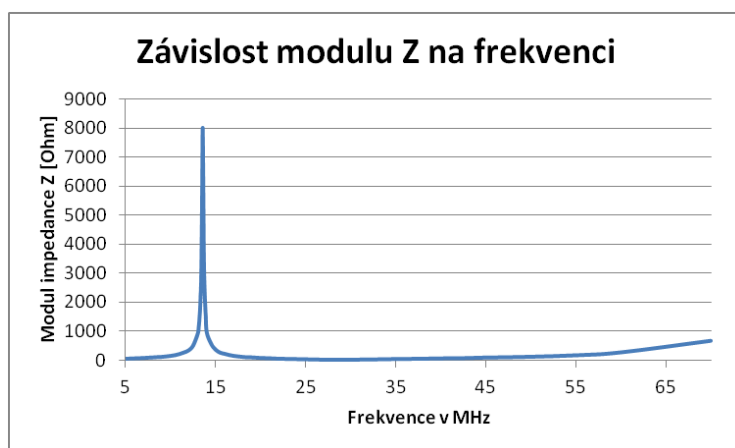
Obrázek 6.5: Porovnání zapojení dvou antén.

Výsledky prvního a druhého měření se poměrně liší, ale stojím si za tím, že obě měření byla prováděna přesně a správně. Tento typ antény je velice náchylný na změny parametrů okolí, hlavně přiblížení ruky. Její položení například na dřevěný stůl výrazně pohlcuje vyzařovaný signál. Tak se chová anténa v laboratorním prostředí. V praktickém zapojení s RFID čtečkou mi to připadalo mnohem stabilnější, hlavně když se nesnažíte realizovat komunikaci na hranici maximálního dosahu. Myslím, že k tomu přispívá i přenos pomocí subnosné vlny.

6.1.1 První měření

Při svém prvním měření, které jsem absolvovala v univerzitní laboratoři hned první den po ukončení vládou nařízené karantény, došlo k nešťastné chybě. Na přípravku s koaxiálním kabelem s SMA konektorem a redukcí na N konektor, kterým jsem chtěla anténu připojit ke spektrálnímu analyzátoru, jsem z neznalosti použila redukcí s jinou impedancí (impedance se na konektor neuvádí), čímž došlo k tomu, že byl v konektoru špatný kontakt a celé toto měření se mi již nepodařilo uskutečnit. Snažila jsem se ale využít drahocenný čas a provést měření tzv. klasickou metodou, pomocí měřiče impedance BM560.

Měření bylo prováděno na jednom z diferenciálních výstupů celé antény s připojenou rezonanční kapacitou (trimr 15pF).

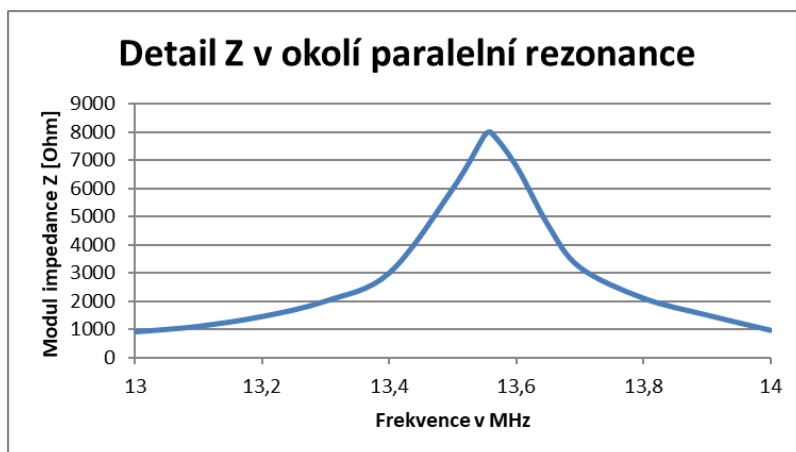


Obrázek 6.6: Závislost modulu Z na frekvenci.

Protože se impedance PRO v těsné blízkosti rezonance blíží k nekonečnu, nemá naměřená hodnota 8000 ohmů žádný vypovídající charakter.

$$\lim_{\omega \rightarrow \omega_0} Z(\omega) = \infty$$

Nedá se z něho vypočítat induktivní reaktance a následně indukčnost antény. Z Thomsonova vztahu pro výpočet rezonanční frekvence by se indukčnost L dala vypočítat jen přibližně, podle rezonanční kapacity. Ale ani tu přesně neznáme. Tento výpočet lze provést vzorcem 3.14.



Obrázek 6.7: Detail Z v okolí paralelní rezonance.

Na frekvenci 28,5 MHz se objevila sériová rezonance indukčnosti s přizpůsobovací kapacitou 12 pF, která se projevila poklesem impedance. Ale fázová charakteristika překrývá jak paralelní, tak i tu sériovou.



Obrázek 6.8: Detail Z v okolí sériové rezonance.



Obrázek 6.9: Závislost fáze na frekvenci.

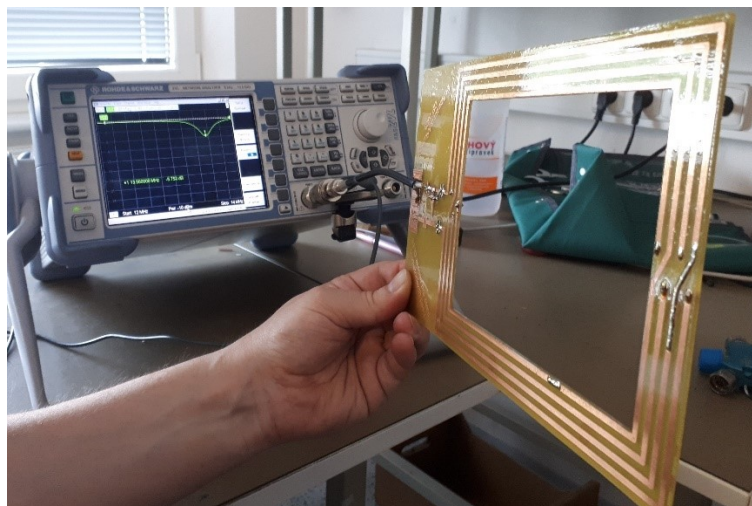
Při sériové rezonanci, kdy by měla být impedance rovna pouze činnému odporu indukčnosti, byla naměřena hodnota $Z = 1,55\Omega$. Přímým měřením digitálním ohmmetrem jsem naměřila $R = 0,65\Omega$.

6.1.2 Druhé měření

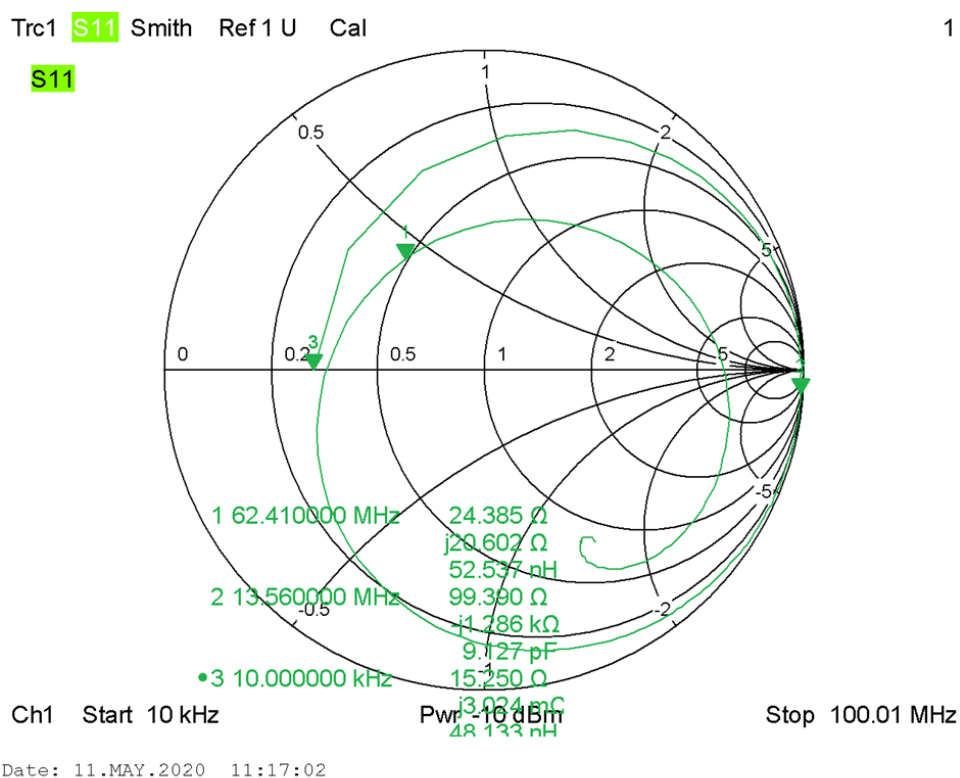
Podruhé se mi povedlo navštívit jedno specializované pracoviště v Pardubicích. Jedná se o firmu ELDIS Pardubice, s.r.o., která se zabývá vývojem a výrobou radiolokační techniky. Svůj čas mi věnoval inženýr z oddělení mikrovln. Mimo jiné mě upozornil na to, že můj N konektor na redukci má 75Ω . Do měřicího přístroje ale patří 50Ω – které mají větší průměr středního kolíku. Díky tomu jsem při měření na univerzitě měla špatný (nebo žádný) kontakt a nepodařilo se mi nic naměřit.

Bohužel nebyla možnost využít měření vyzařovací charakteristiky, protože nebylo jak odstínit anténu od okolního rušení.

U měření jsem použila 20 cm dlouhý koaxiální kabel, který jsem připájela přímo do místa měření. Použitý měřicí přístroj je značky RHODE&SCHWARZ ZVL Vector Network Analyzer, frekvenční rozsah je od 9 kHz do 13,6 GHz.



Obrázek 6.10: Měření rezonance.

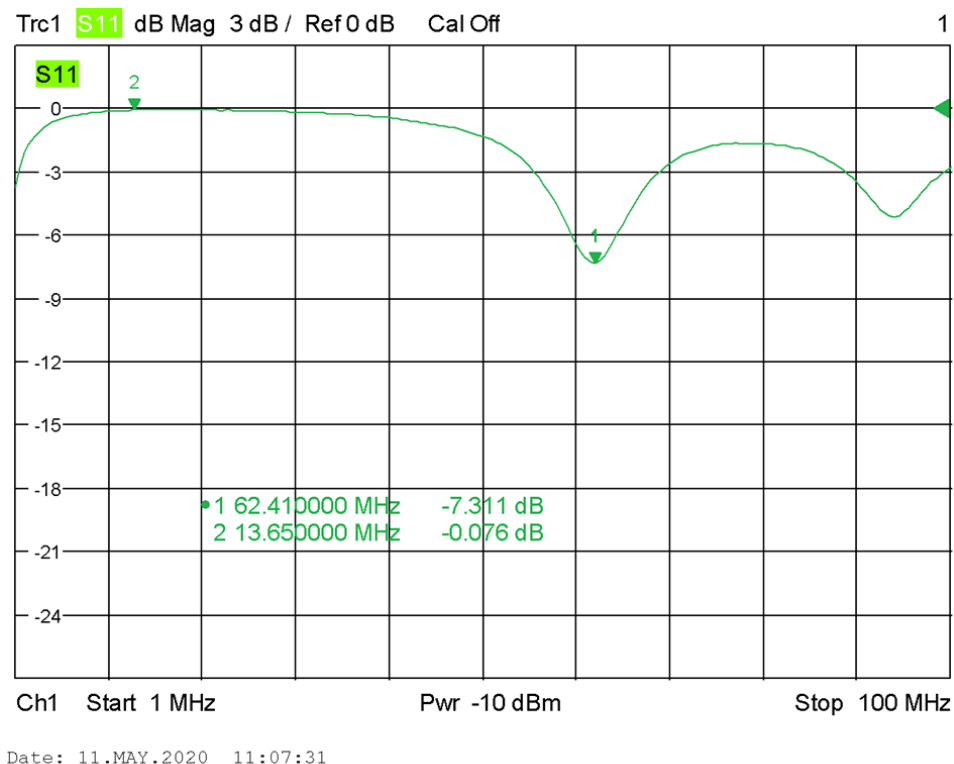


Obrázek 6.11: Širokospektrální měření pouze planární indukčnosti s tlumícími odpory $14,6 \Omega$ ve Smithově zobrazení.

Na Obrázek 6.11 je reálně změřená S_{11} charakteristika samotné planární cívky, která tvoří anténu, včetně sériových odporů určených ke zvýšení jejího reálného odporu. Úmyslně byl

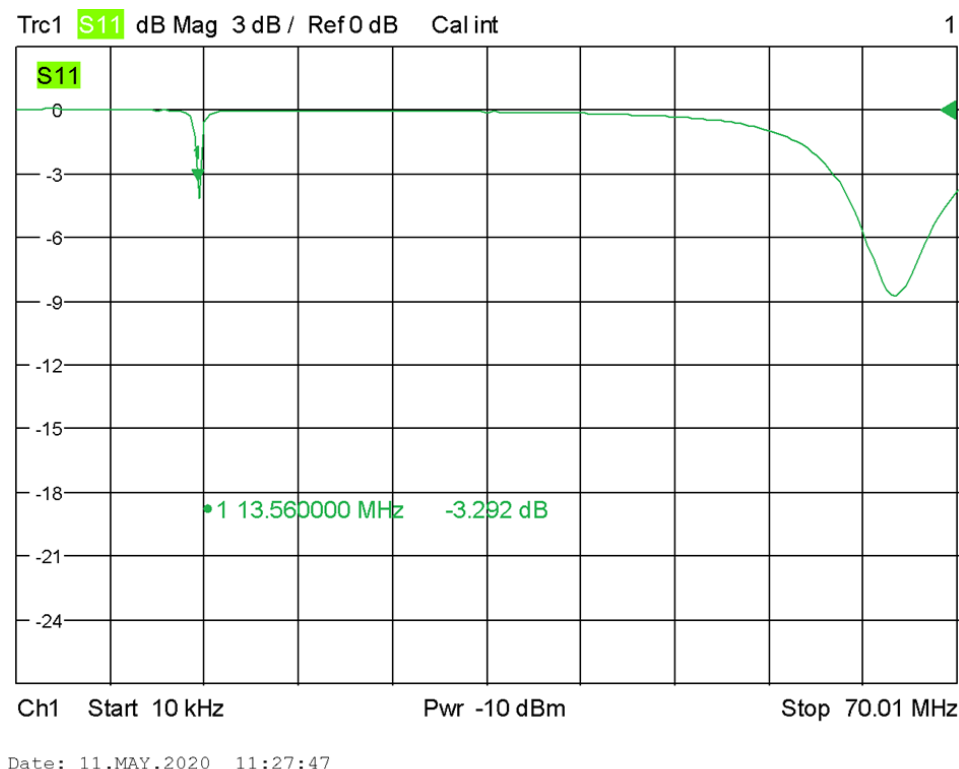
zvolen velký rozsah frekvencí, abych odhalila vlastní rezonance cívky. Jak se ukázalo, je tam takových oblastí více. Může to být způsobeno nevhodnou konstrukcí planární cívky. Je totiž příliš velká a má 4 závity rozložené 3 mm od sebe. Doposud jsem tuto planární indukčnost považovala za součástku se soustředěnými parametry. Z grafu však jasně vyplývá, že se celá cívka chová spíše jako VF vedení s rozloženými parametry, jak je také vidět na Obrázek 3.3.

Je to vlastně několikanásobný RLC článek, který způsobuje, že se ve Smithově diagramu otáčí několikrát dokola v závislosti na frekvenci. Při $f = 10$ kHz (to je nejnižší frekvence nastavitelná na analyzátoru) začíná graf na reálném odporu $2 \cdot 7,3 \, \Omega = 14,6 \, \Omega$ (to je velikost přidáných tlumících odporů). Na konci, při frekvenci 100 MHz, se stáčí již do třetí otáčky.



Obrázek 6.12: Široké spektrum k odhalení vlastních parazitních rezonancí.

Na grafu Obrázek 6.12 jsou vidět vlastní rezonance na 62 MHz a 95 MHz. Parazitní kapacity nelze přesně specifikovat a vzájemně se překrývají.

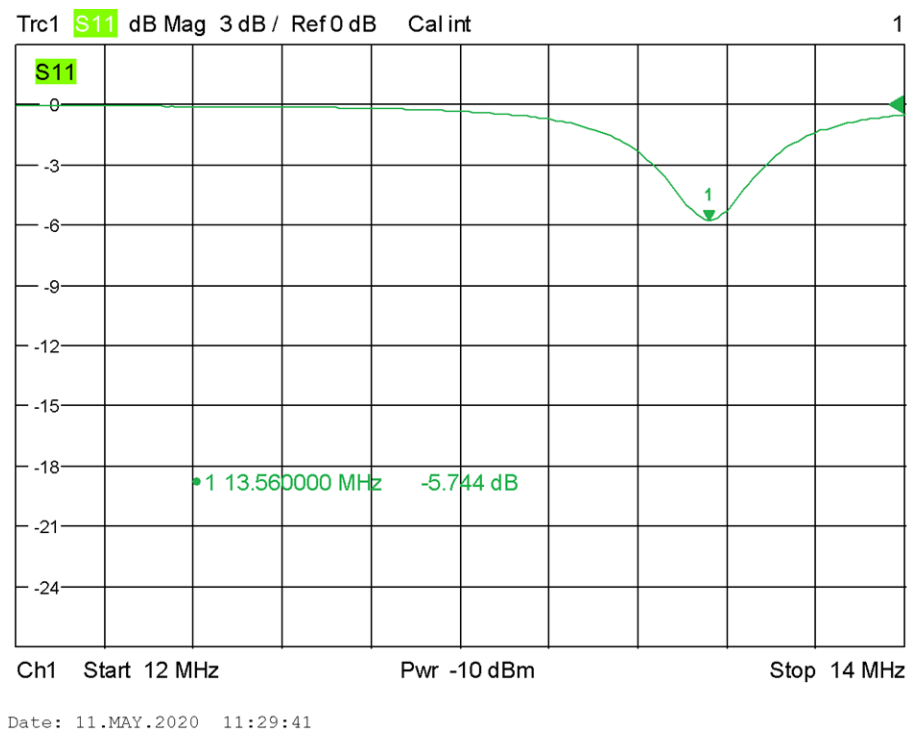


Obrázek 6.13: Širší oblast spektra s laděnou a parazitní rezonancí zároveň.

Druhé měření, Obrázek 6.13, bylo již prováděno na kompletně zapojené anténě (rezonanční a přizpůsobovací kapacity jsou připojeny). Přizpůsobovací kapacita také ovlivňuje rezonanční frekvenci, proto musela být připojena také, jinak by měření nemělo význam.

Na charakteristice je jasně patrný rozdíl v šířce pásma (oproti parazitní rezonanci), protože je rezonance vytvořena pouze jedním kondenzátorem (součástka se soustředěnými parametry). Kromě toho, že je indukčnost úmyslně ztlumená z důvodu snížení jakosti Q tohoto rezonančního obvodu, tak je anténa samozřejmě také špatně impedančně přizpůsobená k měřicímu konektoru 50Ω . To je důvod, proč má amplitudu pouze necelých 6 dB. Z důvodu malého rozlišení tohoto obrázku marker ukazuje méně, následující obrázek je přesnější.

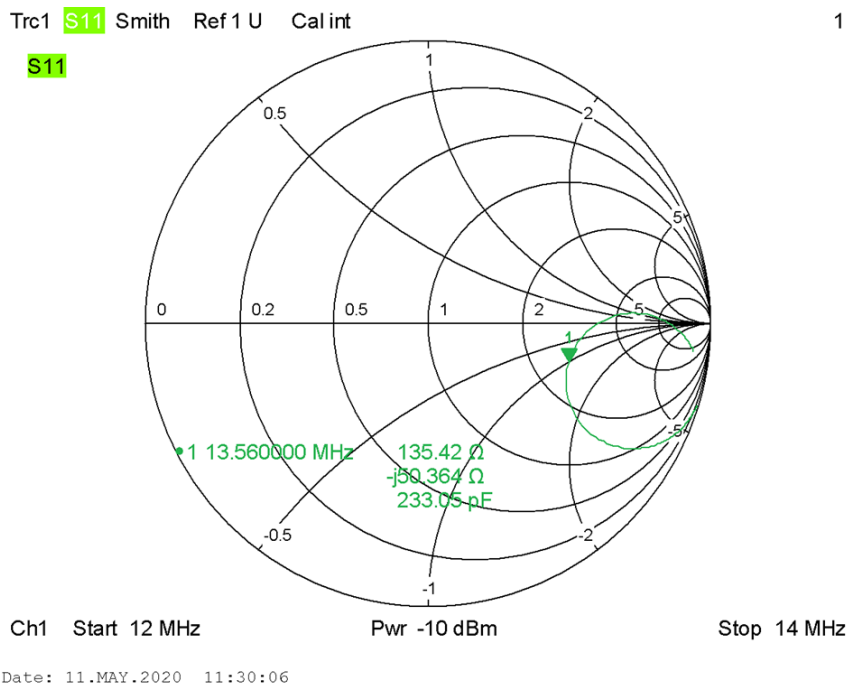
Na Obrázek 6.14 je zobrazený detail rezonanční křivky při 13,56 MHz. Předpokládaná šířka přenášeného pásma B je 400 kHz. Reálné měření je ovlivněno množstvím nedodržených parametrů, hlavně impedančního nepřizpůsobení a také měření pouze jedné poloviny antény.



Obrázek 6.14: Zvětšený detail rezonanční křivky 13,56 MHz.

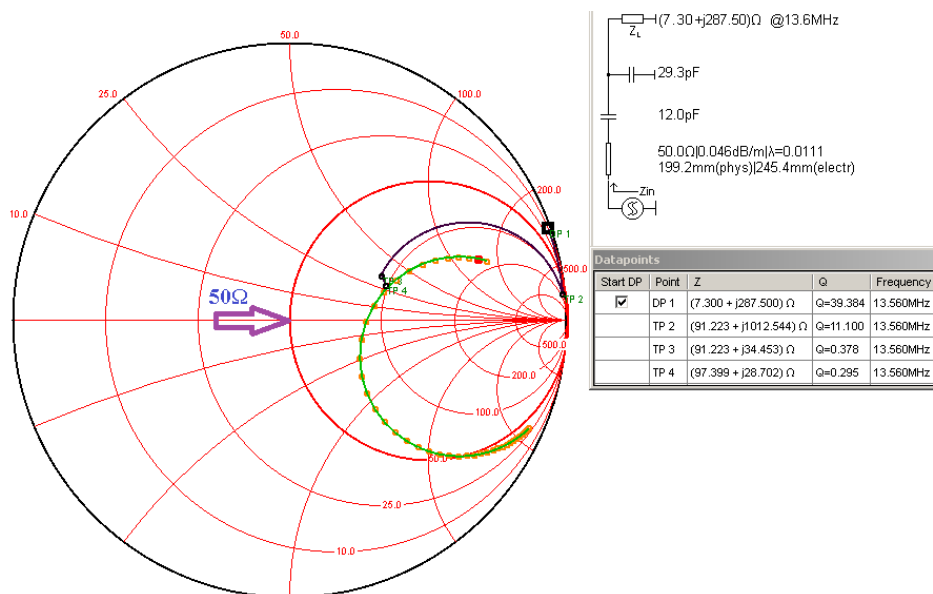
Jelikož spektrální analyzátor s diferenciálním výstupem není běžný, musela jsem měření realizovat provizorně jen s jedním zapojeným vedením. Vycházela jsem z úvahy, že pokud druhý vstup antény zůstane nezapojený, bude se anténa jako PRO chovat podobně, jen bude buzená pouze její polovina. Rezonanční obvod se skládá ze dvou samostatných obvodů s některými společnými částmi. Oba obvody také kmitají na stejné rezonanční frekvenci. Proto ten druhý bude buzený signálem toho prvního a neměl by ho příliš zatěžovat.

Poslední charakteristika na Obrázek 6.15 vyjadřuje skutečnou impedanci antény při frekvenci nosné vlny 13,56 MHz v místě spojení s EMC filtrem. Podle simulace v programu Smith – Obrázek 4.1, jsem předpokládala, že by impedance v tomto bodu (TP-3) měla být $Z_{tr} = (100 + j37) \Omega$. Kromě již uvedených vlivů mi zřejmě velké parazitní kapacity posunuly celý graf až do záporné (čili kapacitní) oblasti, protože naměřená hodnota $Z = (135 - j50) \Omega$. V reálu tyto hodnoty nemají od sebe příliš daleko, protože jen vliv přiblížené ruky k anténě byl značný. Charakteristická kružnice je vytvořena rezonancí obvodu.



Obrázek 6.15: Naměřená S_{11} charakteristika samotné antény ve Smithově zobrazení (zapojen pouze jeden vstup diferenciální antény, druhý je nezatížený). K měření byl použit koaxiální kabel $50\ \Omega$ délky 200 mm.

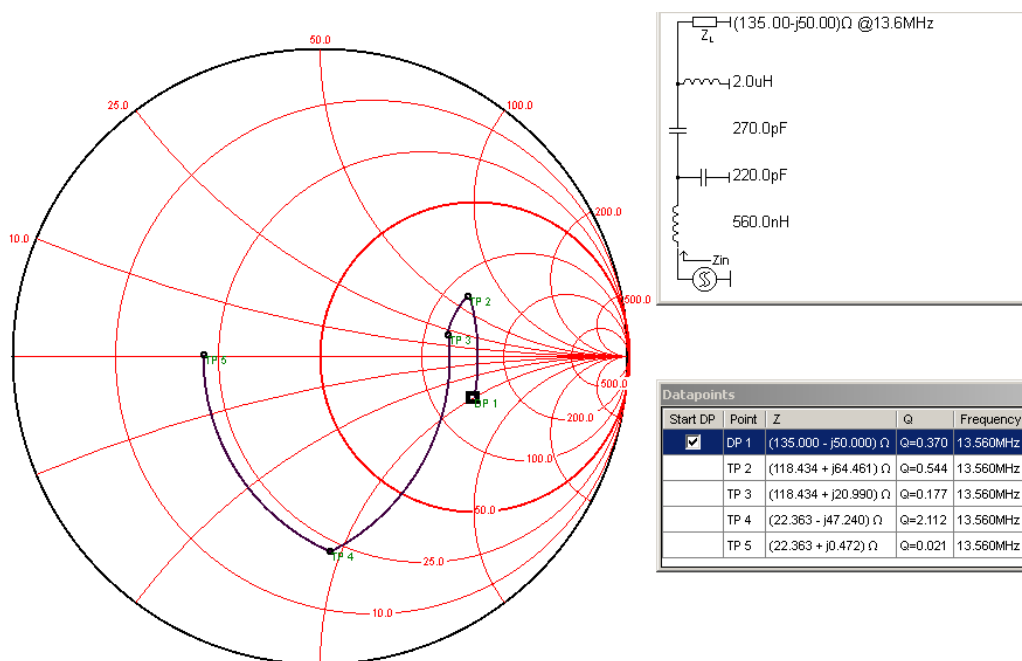
Následující Obrázek 6.16 přikládám pro porovnání s předchozím Obrázek 6.15. Vykreslila jsem S_{11} charakteristiku ve stejném rozsahu frekvencí (12-14) MHz, jako byla měřena spektrálním analyzátozem. Zároveň jsem tam přidala 200 mm koaxiálního kabelu, pomocí kterého bylo prováděno měření. Grafy se liší pouze tím, že ten první je měřen s reálnou indukčností, ale ten druhý je simulovaný s ideální indukčností. Vidíme, že přidání koaxiálního kabelu, jako „vedení s rozloženými parametry“, také stočil S_{11} charakteristiku směrem do kapacitní oblasti. Takovéto vedení způsobuje ve Smithově grafu posun vždy po soustředné kružnici ve směru otáčení hodinových ručiček. A protože planární indukčnost má podobné vlastnosti, tak bude na vině ona.



Obrázek 6.16: Simulovaná S_{11} charakteristika vystihující způsob měření, včetně měřicího kabelu.

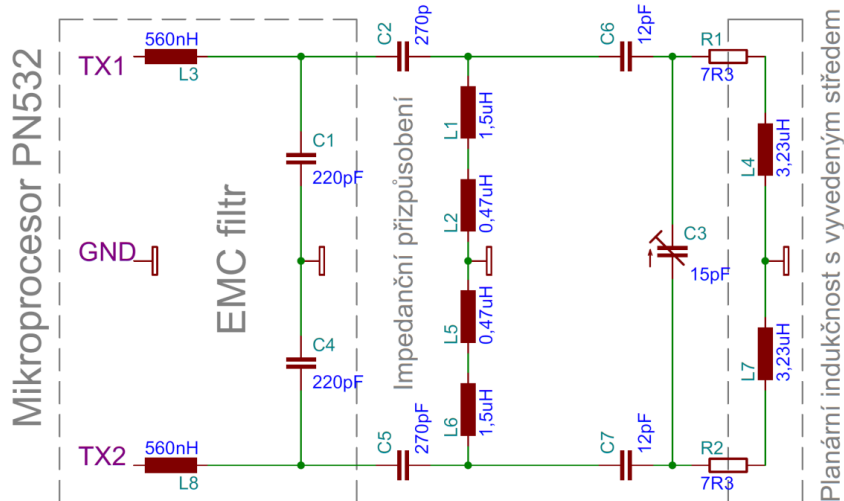
6.2 Návrh kompenzace antény

Na základě výsledků měření jsme se pokusila provést dodatečné impedanční přizpůsobení programem Smith. V místě „živého“ spojení antény s EMC filtrem měla být dle simulace impedance $Z = (99 + j32) \Omega$. Po jejím změření nám však vyšla $(135 - j50) \Omega$.



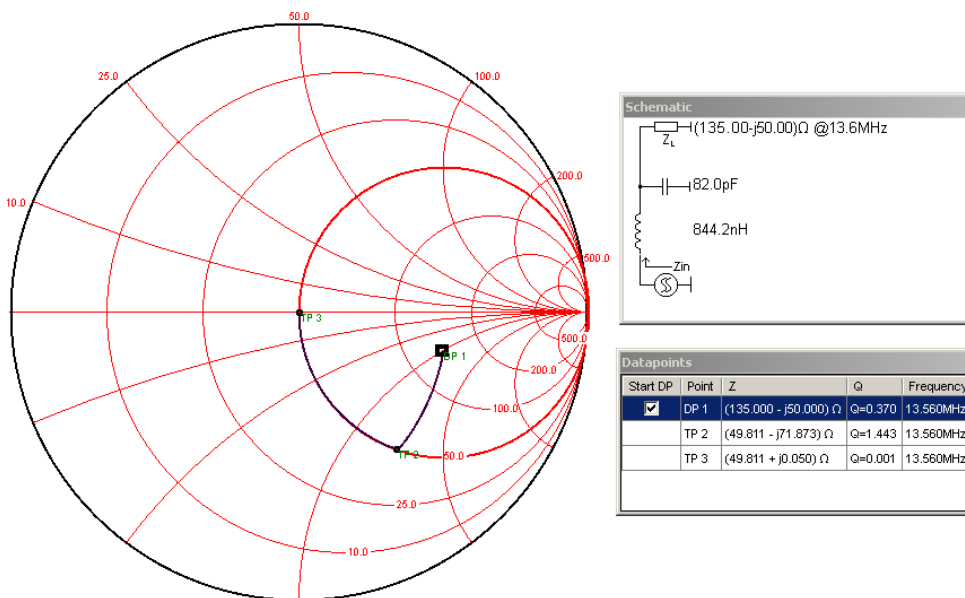
Obrázek 6.17: Náprava posunuté impedance pomocí dvojice LC prvků.

Tím jsem posunula předpokládanou impedanci u výstupu mikroprocesoru na $(23 + j0) \Omega$.

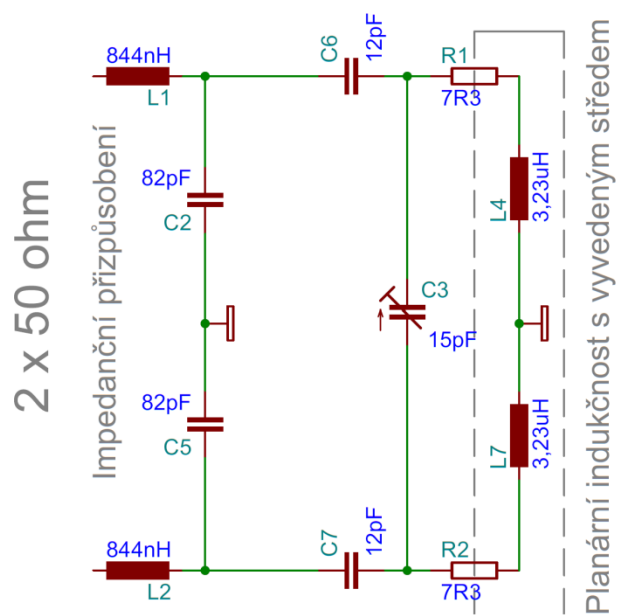


Obrázek 6.18: Celkové upravené zapojení po korekci měřením.

antény.



Obrázek 6.19: Nové doladění na 50 Ω .



Obrázek 6.20: Zapojení pouze vykompenzované antény na připojení ke čtečce 50Ω .

Závěr

Reálné měření mě postavilo před novou realitu. Výpočtem (tím myslím i simulací) nelze nikdy dosáhnout přesného výsledku. Je to přesné počítání s nepřesnými čísly. Protože se reálná planární indukčnost jeví jako prvek s rozloženými parametry, nelze ho přesně zahrnout do simulačních výpočtů. Dlouhou dobu jsem strávila úvahami, za jakých okolností se může indukčnost projevit jako kapacita. Proto, a možná je to i dobře, z této charakteristiky (Obrázek 6.11) nelze vypočítat ani indukčnost. Je to tím, že se planární indukčnost chová jako vedení. To se ve Smithově diagramu projevuje tak, že se v závislosti na frekvenci pohybuje po soustředné kružnici, resp. po spirále, okolo středu. Čili pravidelně prochází všemi kvadranty. To je také důvod doporučení, že by RFID anténa měla mít maximálně 3 μH , což jsem nedodržela a postavila 6,75 μH . Snížením indukčnosti na polovinu by se snížil počet závitů a tím i jejich vzájemné parazitní kapacity.

Navzdory tomu, že mé měření obsahuje i několik sporných míst, tak jsem spokojená s reálnou komunikací. Na místě biometrického pasu jsem použila náhradu – MIFARE ID kartu, protože zabezpečené cestovní doklady vyžadují ke komunikaci speciální SW, který nemám, ale možná i HW. Není totiž vyloučené, že mikročip PN532 má v sobě z bezpečnostních důvodů naimplementovanou SW ochranu proti jeho možnému zneužívání.

Sériová rezonance z prvního měření se v druhém měření sice nijak neprojevila, ale možná jsem jen špatně hledala. Rozdíl mezi sériovou a paralelní rezonancí totiž spočívá v impedanci, kterou spektrální analyzátor měří. A protože má měřený graf na Obrázek 6.12 jedno společné měřítko, tak se rozdíl mezi 8 $\text{k}\Omega$ a 1,55 Ω může ztrácet v rozlišení obrázku.

Nejedná se o klasickou anténu a její využití je pouze v jejím blízkém poli. Prioritou je ale nezpochybnitelný dosah cca do 50 mm a spolehlivý přenos dat. Nadměrný dosah je naopak nežádoucí a zneužitelný. Při exaktním měření se často vyskytují problémy s vnějšími vlivy. Vlastnosti antény jsou přímo ovlivňovány blízkými objekty jako je kapacita lidské ruky nebo okolního prostředí. Při reálném použití to však nemusí mít takový dopad, a to hlavně díky již prověřené technologii RFID čteček. Má anténa je předurčena jako součást optického snímače strojově čitelných údajů. Proto cestovní doklad musí být přiložen těsně k průzračné ploše a tím se dostane do zaručeného dosahu.

Použitá literatura

- [1] *INTERNATIONAL STANDARD ISO/IEC14443-2* [online]., 17 [cit. 2020-01-10]. Dostupné z: <http://www.emutag.com/iso/14443-2.pdf>.
- [2] FINKENZLLER, Klaus. *RFID Handbook FUNDAMENTALS ANDAPPLICATIONS IN CONTACTLESSSMART CARDS, RADIO FREQUENCYIDENTIFICATION AND NEAR-FIELDCOMMUNICATION, THIRD EDITION*. A John Wiley and Sons, Ltd., Publication, 2010. ISBN 978-0-470-69506-7.
- [3] *RFID Qualification Network: Matching Networks* [online]. In: DIPL.-ING. DR. MICHAEL GEBHART, MSC. [cit. 2020-01-07]. Dostupné z: http://rfid-systems.at/04_Matching_Networks.pdf
- [4] *Antenna design guide for MFRC52x, PN51x and PN53x* [online]. ©NXP B.V. 2010. All rights reserved, 2010 [cit. 2020-02-25]. Dostupné z: <https://my.eng.utah.edu/~mlewis/ref/NFC/AN1445.pdf>
- [5] *PN532/C1, Near Field Communication controller* [online]. Product data sheet COMPANY PUBLIC, 2017 [cit. 2020-01-28]. Dostupné z: https://www.nxp.com/docs/en/nxp/data-sheets/PN532_C1.pdf
- [6] *MIFARE Classic as NFC Type MIFARE Classic Tag* [online]. Application note COMPANY PUBLIC, 2012 [cit. 2020-01-28]. Dostupné z: <https://www.nxp.com/docs/en/application-note/AN1305.pdf>
- [7] *Smith-Chart Software and Related Documents: Fritz Dellsperger* [online]. Fritz Dellsperger, 2018 [cit. 2020-01-28]. Dostupné z: <https://www.fritz.dellsperger.net/smith.html>
- [8] *Flexible RG58 Coax Cable Single Shielded with Black PVC (NC) Jacket: RF Cables Technical Data Sheet* [online]. Pasternack Enterprises, 2017 [cit. 2020-01-28]. Dostupné z: <https://www.pasternack.com/images/ProductPDF/RG58C-U.pdf>
- [9] *Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards* [online]. ATMEL Corporation [cit. 2020-01-28]. Dostupné z: <https://www.scribd.com/document/352276538/doc2056-pdf>
- [10] *INTERNATIONALSTANDARD ISO/IEC14443-3: Identification cards — Contactlessintegrated circuit(s) cards — Proximitycards — Part 3: Initialization and anticollision* [online]. 2001 [cit. 2020-01-28]. Dostupné z: https://www.academia.edu/28197214/ISO_IEC_14443-3
- [11] *Telekomunikační systémy v širokém spektru: MLA Magnetic Loop Antenna* [online]. B PLUS TV [cit. 2019-12-08]. Dostupné z: <https://www.btv.cz/en/MLA-magnetic-loop-antenna>

- [12] MELEZÍNEK, Adolf. *Elektronika: Pro 3. a 4. ročník SPŠ elektrotechnických*. Státní nakladatelství technické literatury, 1970. ISBN 978-80-03-00102-6.
- [13] *International Civil Aviation Organization: El Rol de la OACI Dentro del Marco Global de DVLM y eDVLM* [online]. Regional Officer Aviation Security and Facilitation NACC Office, 2013 [cit. 2019-12-09]. Dostupné z: <http://clacsec.lima.icao.int/Reuniones/2013/3raFALAVSEC-Reg/Presentaciones/2.5%20Rol%20OACI%20dentro%20del%20Marco%20Global%20de%20DVLM%20y%20eDVLM.rev.pdf>
- [14] *Cybersecurity & Wireless Technology Expert: RFID Pickpocketing Debunked* [online]. [cit. 2019-12-09]. Dostupné z: <https://scottschober.com/rfid-pickpocketing-debunked/>
- [15] *Fotos der Welt: Nikola Tesla* [online]. 2017 [cit. 2019-12-20]. Dostupné z: <https://www.diefotografen.de/2017/09/14/nikola-tesla/>
- [16] Jean-Marc Laheurte, Christian Ripoll, Dominique Paret a Christophe Loussert. *UHF RFID Technologies for Identification and Traceability*. John Wiley & Sons, 2014. ISBN 9781118930939.
- [17] *CIRCUIT DESIGN: RFID* [online]. 2012 [cit. 2019-12-20]. Dostupné z: <https://blog.mbedded.ninja/electronics/circuit-design/rfid/>
- [18] *Antény pro systémy RFID* [online]. Ústav mikroelektroniky, FEKT VUT: Ing. Tomáš Procházka, 2002 [cit. 2019-10-15]. Dostupné z: <http://www.elektrorevue.cz/clanky/02022/index.html>
- [19] *SOS electronic: Technologie NFC v 7 bodech* [online]. 2019 [cit. 2019-10-16]. Dostupné z: <https://www.soselectronic.cz/articles/no-name/technologie-nfc-v-7-bodech-2281>
- [20] Samuraj-cz: *Bezkontaktní čipové technologie a přístupové systémy* [online]. 2019 [cit. 2019-11-22]. Dostupné z: <https://www.samuraj-cz.com/clanek/bezkontaktni-cipove-technologie-a-pristupove-systemy/>
- [21] Wiki for ITS: *Components of the RFID System* [online]. University of Oslo [cit. 2019-11-30]. Dostupné z: https://its-wiki.no/images/a/af/Components_of_the_RFID_System.pdf
- [22] Harvey, Lehpamer. *RFID Design Principles: Components of the RFID System* [online]. 2012 [cit. 2019-11-30]. Dostupné z: https://its-wiki.no/images/a/af/Components_of_the_RFID_System.pdf
- [23] *Software development: Jak funguje biometrický pas* [online]. 2015 [cit. 2019-09-05]. Dostupné z: <https://blog.zvestov.cz/software%20development/2015/12/15/jak-funguje-biometricky-pas.html>
- [24] *MIFARE Classic EV1 4K - Mainstream contactless smart cardIC for fast and easy solution development: Product data sheet* [online]. NXP Semiconductor,

23November2017. [cit. 2019-09-05]. Dostupné z: https://www.nxp.com/docs/en/data-sheet/MF1S70YYX_V1.pdf

- [25] *Arduino Parts & Projects: PN532 NFC RFID module for Arduino* [online]. 2017 [cit. 2019-09-24]. Dostupné z: <https://osoyoo.com/2017/07/19/pn532-nfc-rfid-module-for-arduino/>

Seznam příloh

Příloha A:	Naměřené hodnoty	I
------------	------------------------	---

Příloha A: *Naměřené hodnoty*

Tabulka A.1: *Tabulka naměřených hodnot prvního měření*

číslo měře	f[Mhz]	Z[W]	Fi[°]	číslo měře	f[Mhz]	Z[W]	Fi[°]
1	5,00	41,0	90,0	43	20,50	62,0	-88,0
2	5,50	48,0	90,0	44	21,00	56,0	-86,0
3	6,00	53,0	90,0	45	21,50	50,0	-86,0
4	6,50	60,0	90,0	46	22,00	40,0	-86,0
5	7,00	68,0	90,0	47	22,50	39,0	-86,0
6	7,50	78,0	90,0	48	23,00	32,0	-86,0
7	8,00	87,0	90,0	49	23,50	30,0	-84,0
8	8,50	98,0	90,0	50	24,00	28,0	-84,0
9	9,00	105,0	90,0	51	24,50	24,2	-83,0
10	9,50	120,0	90,0	52	25,00	20,6	-82,0
11	10,00	140,0	90,0	53	25,50	17,5	-81,0
12	10,50	165,0	90,0	54	26,00	14,0	-79,0
13	11,00	205,0	90,0	55	26,50	11,0	-78,0
14	11,50	260,0	90,0	56	27,00	8,0	-74,0
15	12,00	330,0	90,0	57	27,50	6,1	-69,0
16	12,50	500,0	88,0	58	28,00	3,2	-56,0
17	13,00	900,0	85,0	59	28,50	1,7	-14,0
18	13,10	1100,0	83,5	60	28,59	1,6	0,0
19	13,20	1450,0	82,0	61	29,00	2,4	55,0
20	13,30	2000,0	78,0	62	29,50	4,8	75,0
21	13,40	3000,0	70,0	63	30,00	7,0	82,0
22	13,50	6000,0	42,0	64	30,50	9,4	87,0
23	13,55	7900,0	9,0	65	31,00	11,0	90,0
24	13,56	8000,0	0,0	66	31,50	13,0	90,0
25	13,60	6800,0	-32,0	67	32,00	15,0	90,0
26	13,65	4700,0	-52,0	68	32,50	18,0	90,0
27	13,70	3200,0	-64,0	69	33,00	20,0	90,0
28	13,80	2100,0	-75,0	70	33,50	22,5	90,0
29	13,90	1500,0	-79,0	71	34,00	25,0	90,0
30	14,00	960,0	-82,0	72	34,50	27,0	90,0
31	14,50	550,0	-85,0	73	35,00	29,5	90,0
32	15,00	350,0	-88,0	74	36,00	31,0	90,0
33	15,50	250,0	-88,0	75	37,00	38,0	90,0
34	16,00	210,0	-88,0	76	38,00	41,0	90,0
35	16,50	170,0	-89,0	77	39,00	46,0	90,0
36	17,00	140,0	-89,0	78	40,00	52,0	90,0
37	17,50	120,0	-89,0	79	43,00	64,0	90,0
38	18,00	105,0	-89,0	80	45,00	80,0	90,0
39	18,50	90,0	-89,0	81	50,00	108,0	90,0
40	19,00	87,0	-89,0	82	55,00	160,0	90,0
41	19,50	78,0	-89,0	83	60,00	260,0	90,0
42	20,00	69,0	-89,0	84	70,00	660,0	90,0